FIG. 1

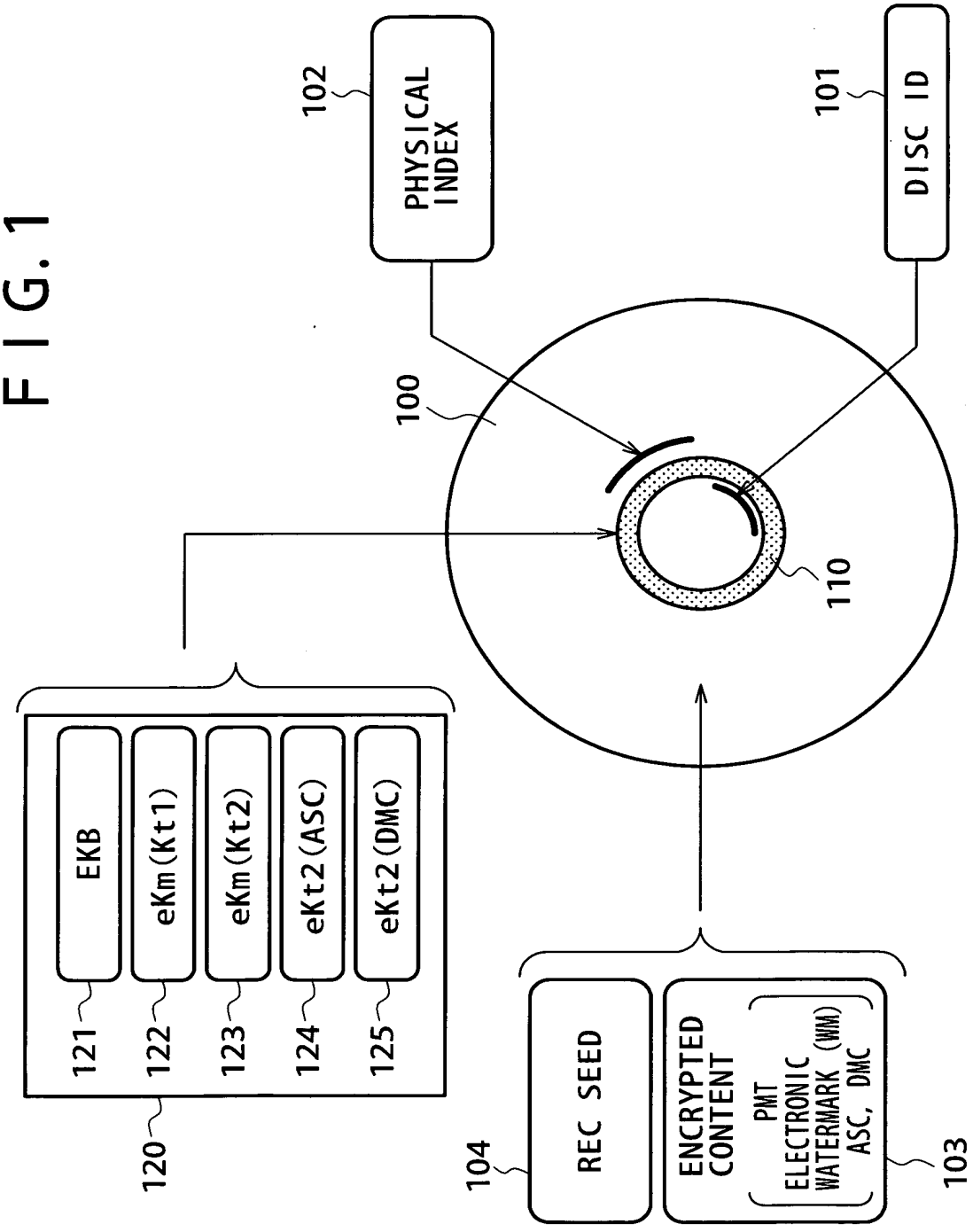

102
PHYSICAL INDEX
101
DISC ID
100
110
EKB
eKm(Kt1)
eKm(Kt2)
eKt2(ASC)
eKt2(DMC)
121
122
123
124
125
120
REC SEED
104
ENCRYPTED CONTENT
PMT
ELECTRONIC WATERMARK (WM)
ASC, DMC
103

FIG. 2

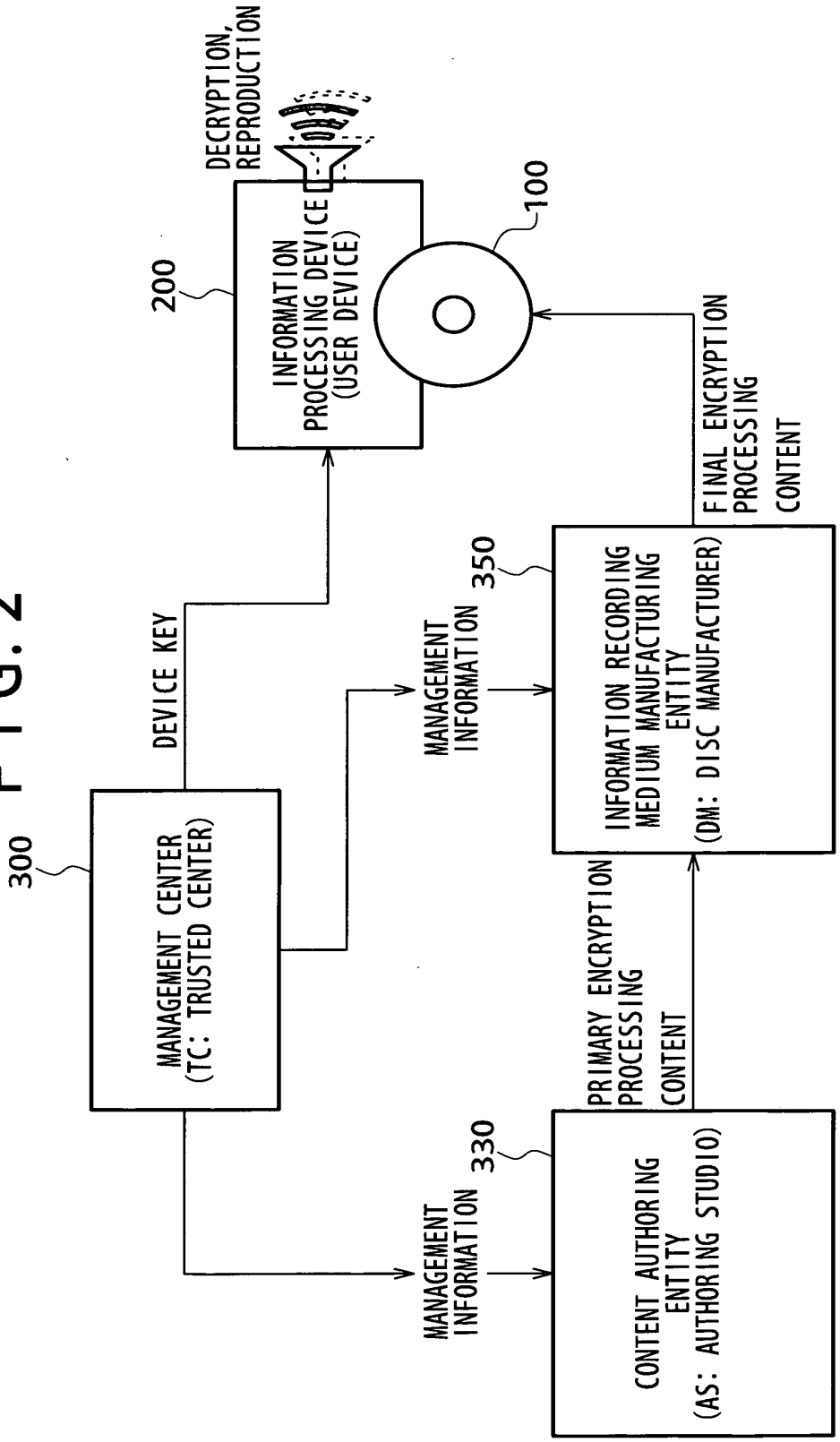

300
MANAGEMENT CENTER
(TC: TRUSTED CENTER)
DEVICE KEY
MANAGEMENT INFORMATION
MANAGEMENT INFORMATION
330
CONTENT AUTHORING ENTITY
(AS: AUTHORING STUDIO)
PRIMARY ENCRYPTION PROCESSING CONTENT
350
INFORMATION RECORDING MEDIUM MANUFACTURING ENTITY
(DM: DISC MANUFACTURER)
FINAL ENCRYPTION PROCESSING CONTENT
100
200
INFORMATION PROCESSING DEVICE
(USER DEVICE)
DECRYPTION, REPRODUCTION

FIG. 3

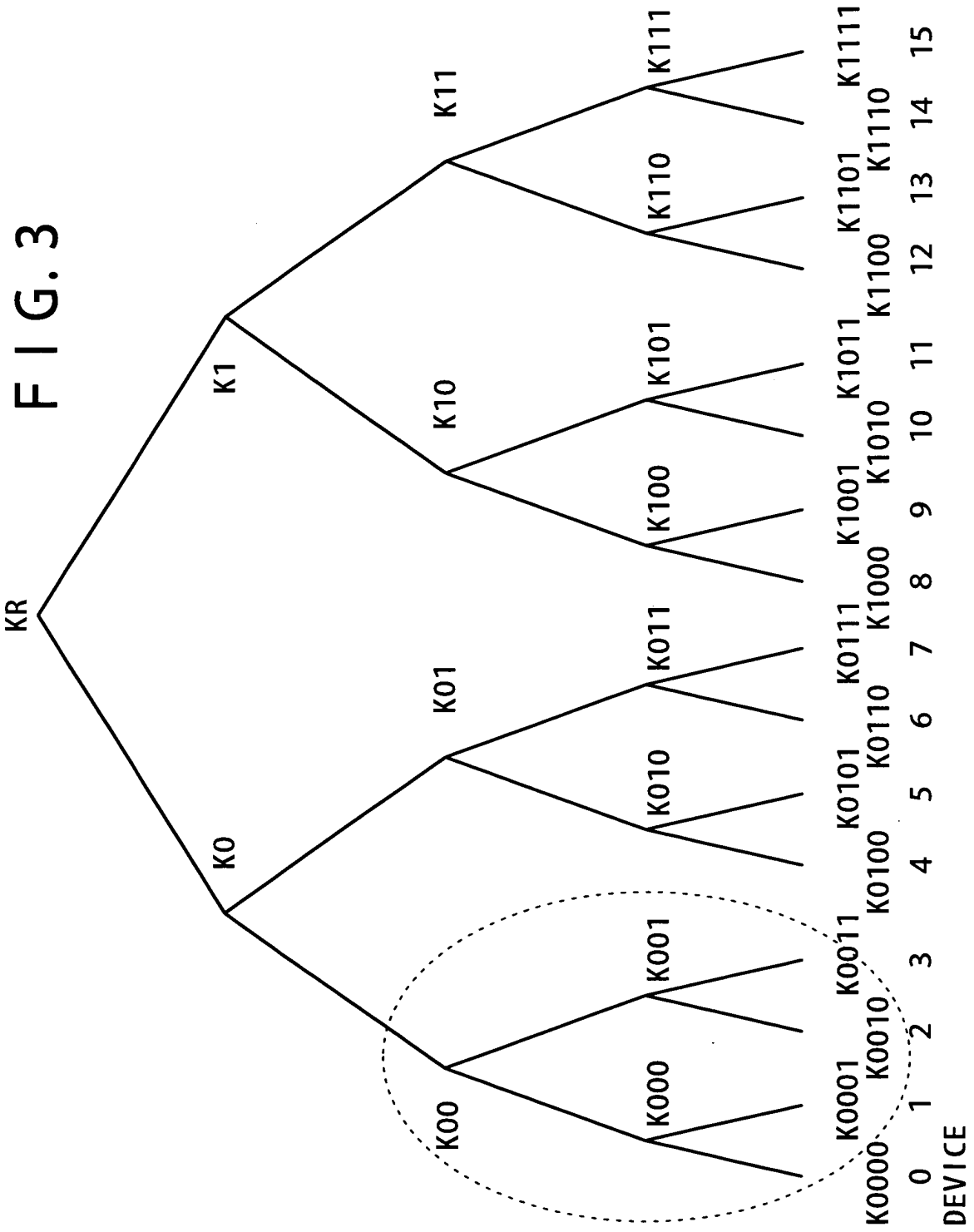

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
DEVICE

FIG. 4

(A) EKB (ENABLING KEY BLOCK)
EXAMPLE 1

SEND NODE KEY OF VERSION t TO DEVICES 0, 1, 2.

VERSION t	
INDEX	ENCRYPTED KEY
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

(B) EKB (ENABLING KEY BLOCK)
EXAMPLE 2

SEND NODE KEY OF VERSION t TO DEVICES 0, 1, 2.

VERSION t	
INDEX	ENCRYPTED KEY
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

Oblon, Spivak, et al.
703-413-3000
Docket # 280760US
Sheet 4 of 27

FIG. 5

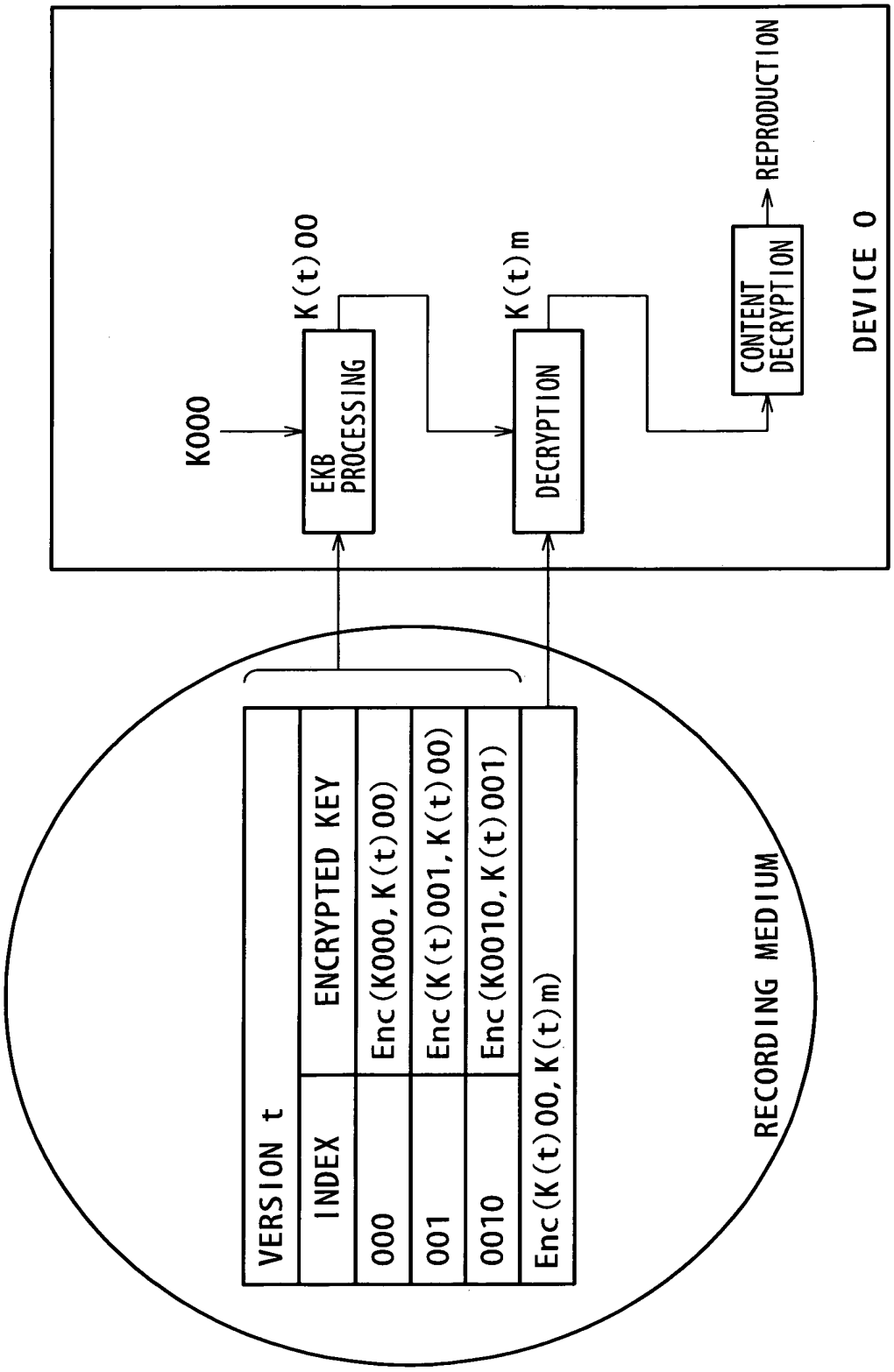

DEVICE 0
K000
EKB PROCESSING
K(t)00
DECRYPTION
K(t)m
CONTENT DECRYPTION
REPRODUCTION
RECORDING MEDIUM
VERSION t
INDEX
ENCRYPTED KEY
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)m)

FIG. 6

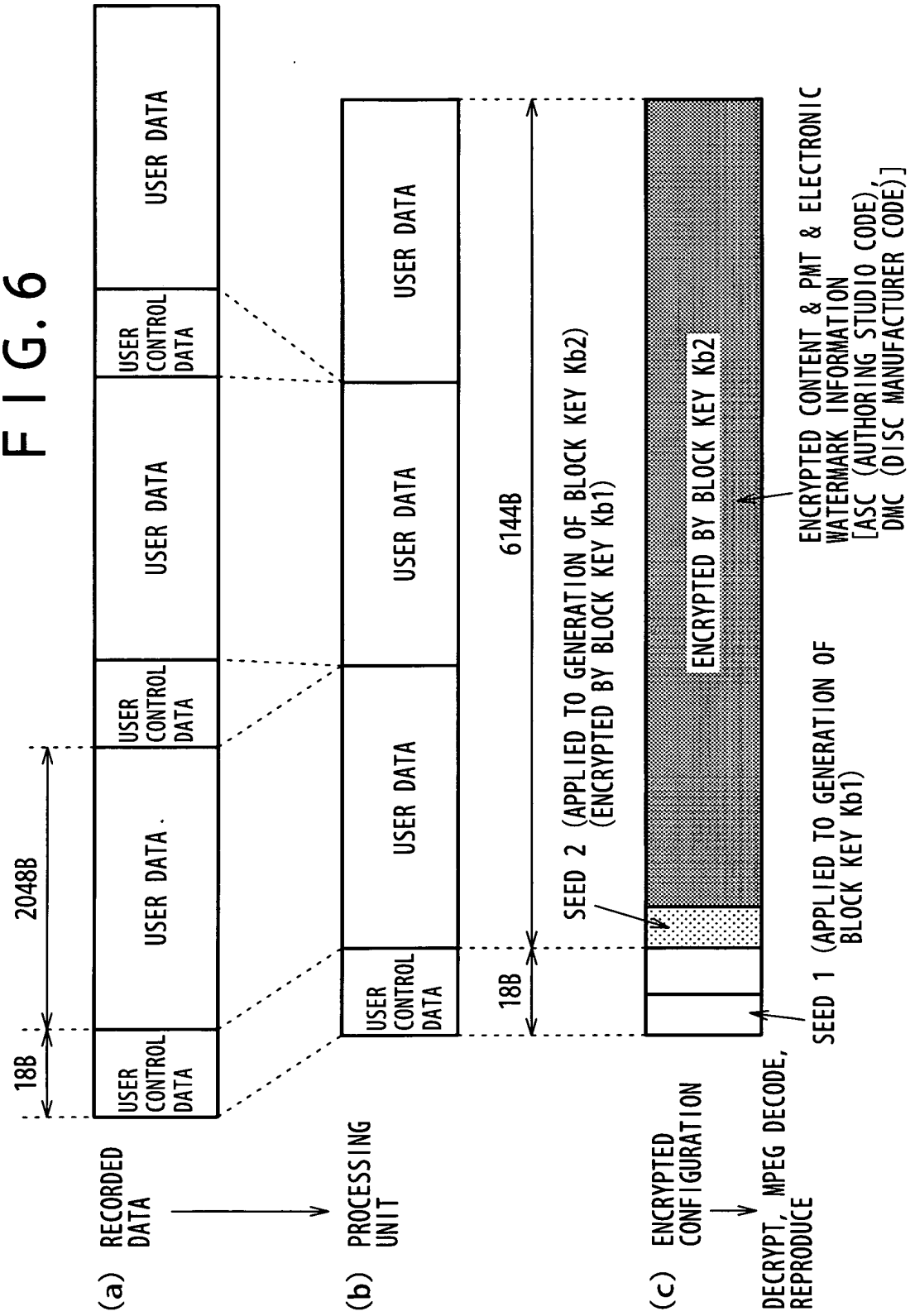

(a) RECORDED DATA
(b) PROCESSING UNIT
(c) ENCRYPTED CONFIGURATION
DECRYPT, MPEG DECODE, REPRODUCE
18B
2048B
USER CONTROL DATA
USER DATA
6144B
SEED 2 (APPLIED TO GENERATION OF BLOCK KEY Kb2) (ENCRYPTED BY BLOCK KEY Kb1)
ENCRYPTED BY BLOCK KEY Kb2
ENCRYPTED CONTENT & PMT & ELECTRONIC WATERMARK INFORMATION [ASC (AUTHORING STUDIO CODE), DMC (DISC MANUFACTURER CODE)]
SEED 1 (APPLIED TO GENERATION OF BLOCK KEY Kb1)

FIG. 7

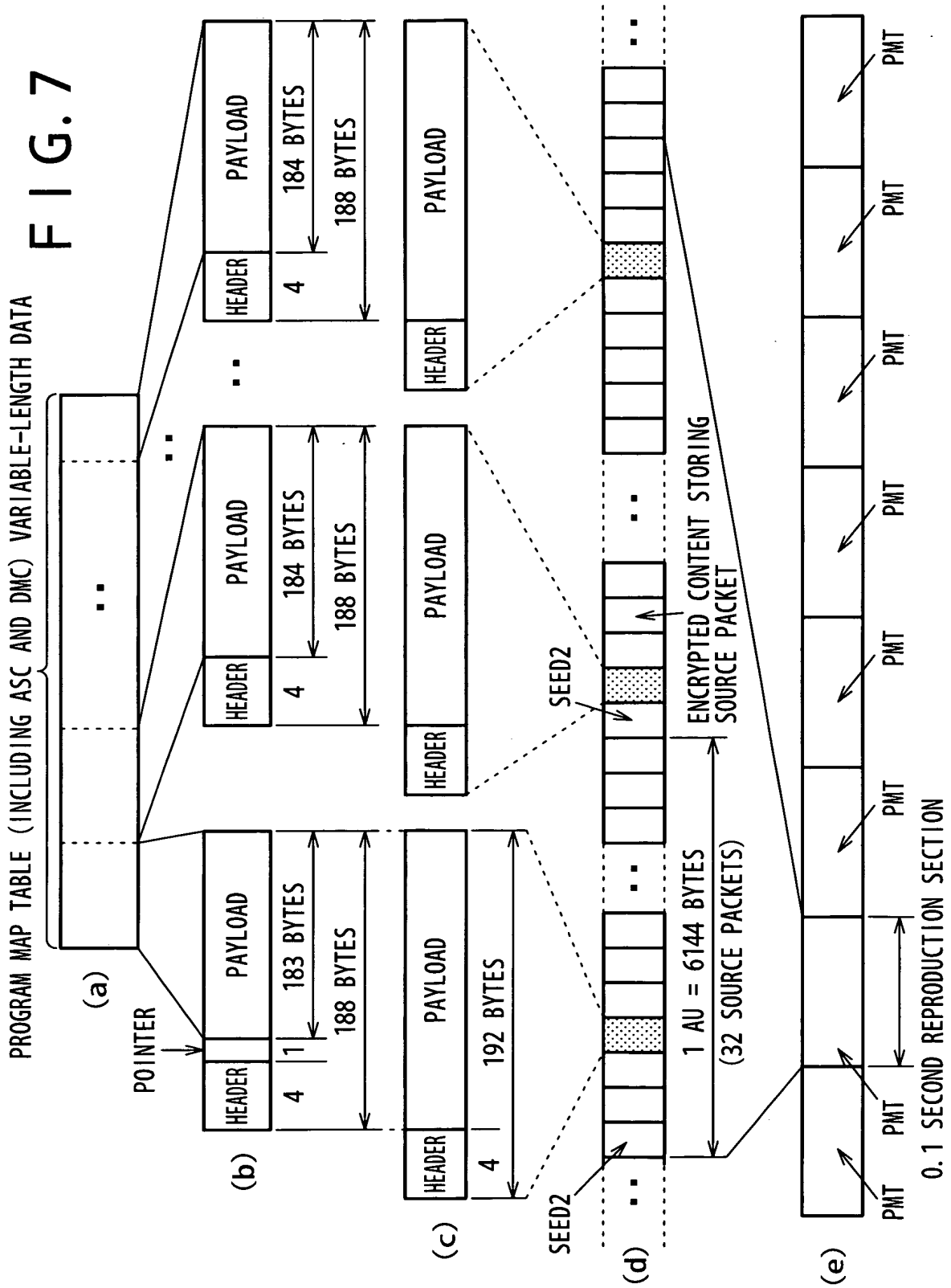

PROGRAM MAP TABLE (INCLUDING ASC AND DMC) VARIABLE-LENGTH DATA
(a)
POINTER
HEADER
PAYLOAD
4
1
183 BYTES
188 BYTES
184 BYTES
192 BYTES
(b)
(c)
SEED2
ENCRYPTED CONTENT STORING SOURCE PACKET
1 AU = 6144 BYTES
(32 SOURCE PACKETS)
(d)
PMT
(e)
0.1 SECOND REPRODUCTION SECTION

FIG. 8

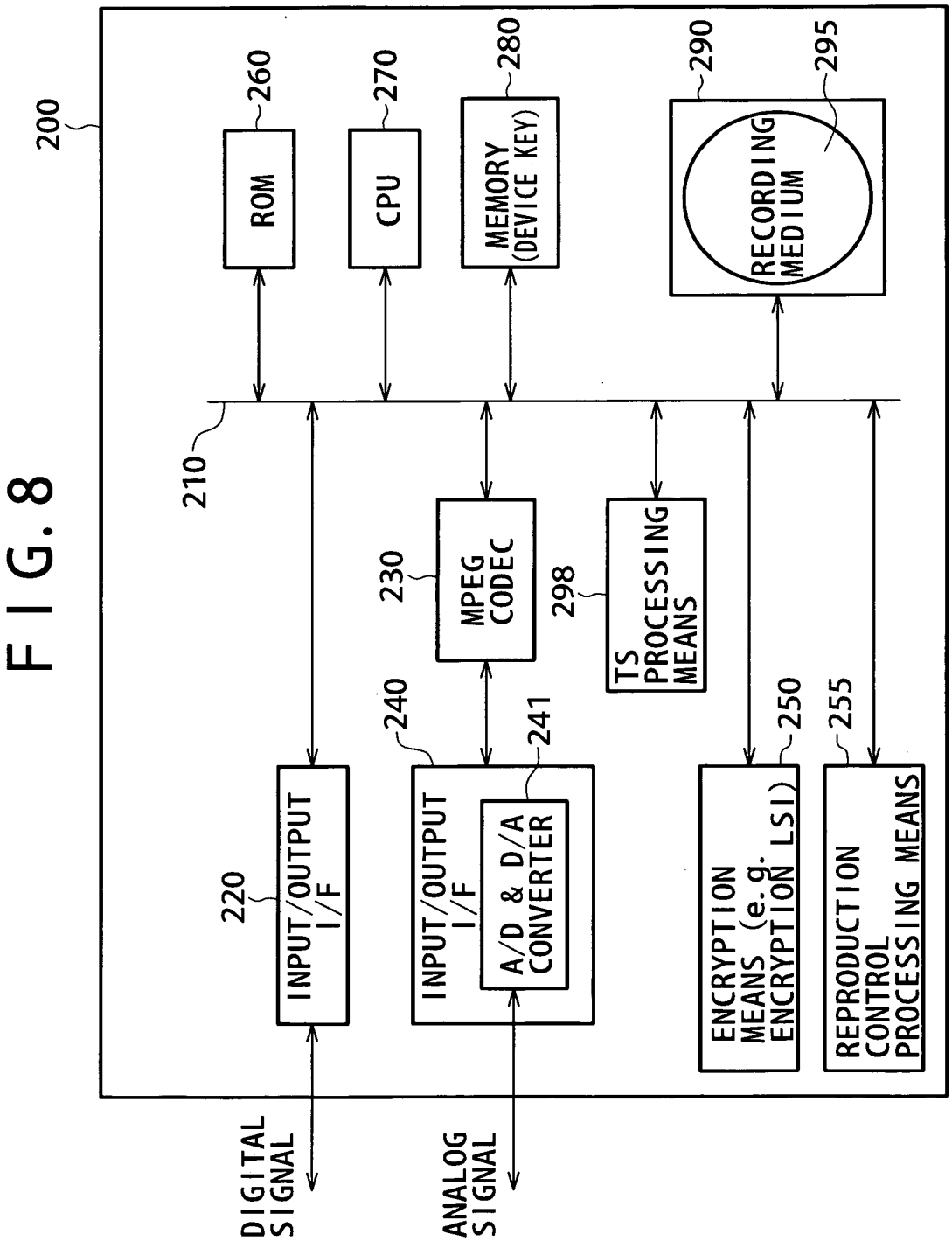

200
260
ROM
270
CPU
280
MEMORY (DEVICE KEY)
290
295
RECORDING MEDIUM
210
230
MPEG CODEC
298
TS PROCESSING MEANS
240
241
250
255
220
INPUT/OUTPUT I/F
INPUT/OUTPUT I/F
A/D & D/A CONVERTER
ENCRYPTION MEANS (e.g. ENCRYPTION LSI)
REPRODUCTION CONTROL PROCESSING MEANS
DIGITAL SIGNAL
ANALOG SIGNAL

FIG. 9

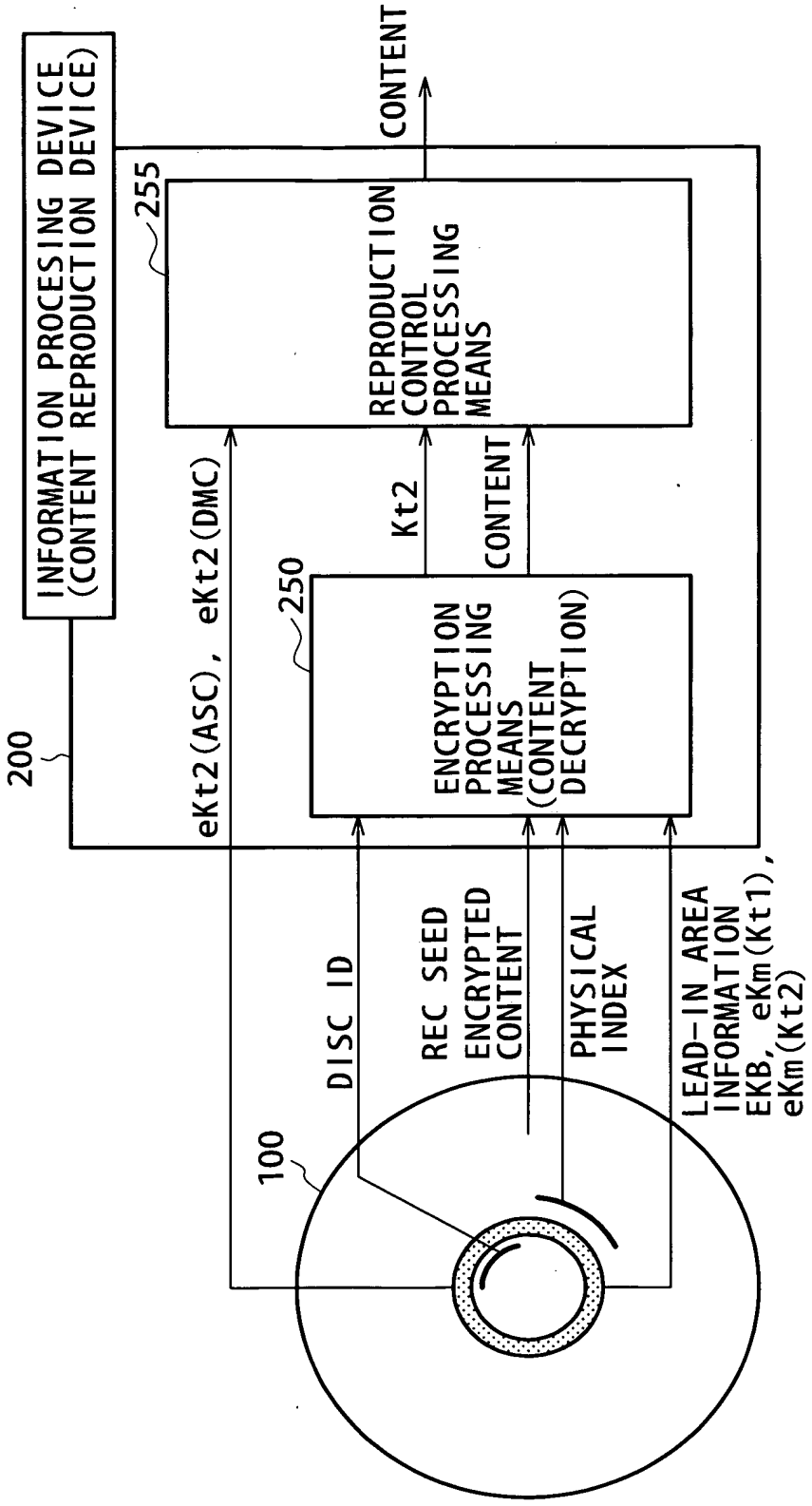

INFORMATION PROCESING DEVICE
(CONTENT REPRODUCTION DEVICE)
200
255
REPRODUCTION CONTROL PROCESSING MEANS
CONTENT
250
ENCRYPTION PROCESSING MEANS (CONTENT DECRYPTION)
Kt2
CONTENT
eKt2(ASC), eKt2(DMC)
100
DISC ID
REC SEED
ENCRYPTED CONTENT
PHYSICAL INDEX
LEAD-IN AREA INFORMATION
EKB, eKm(Kt1),
eKm(Kt2)

FIG. 10

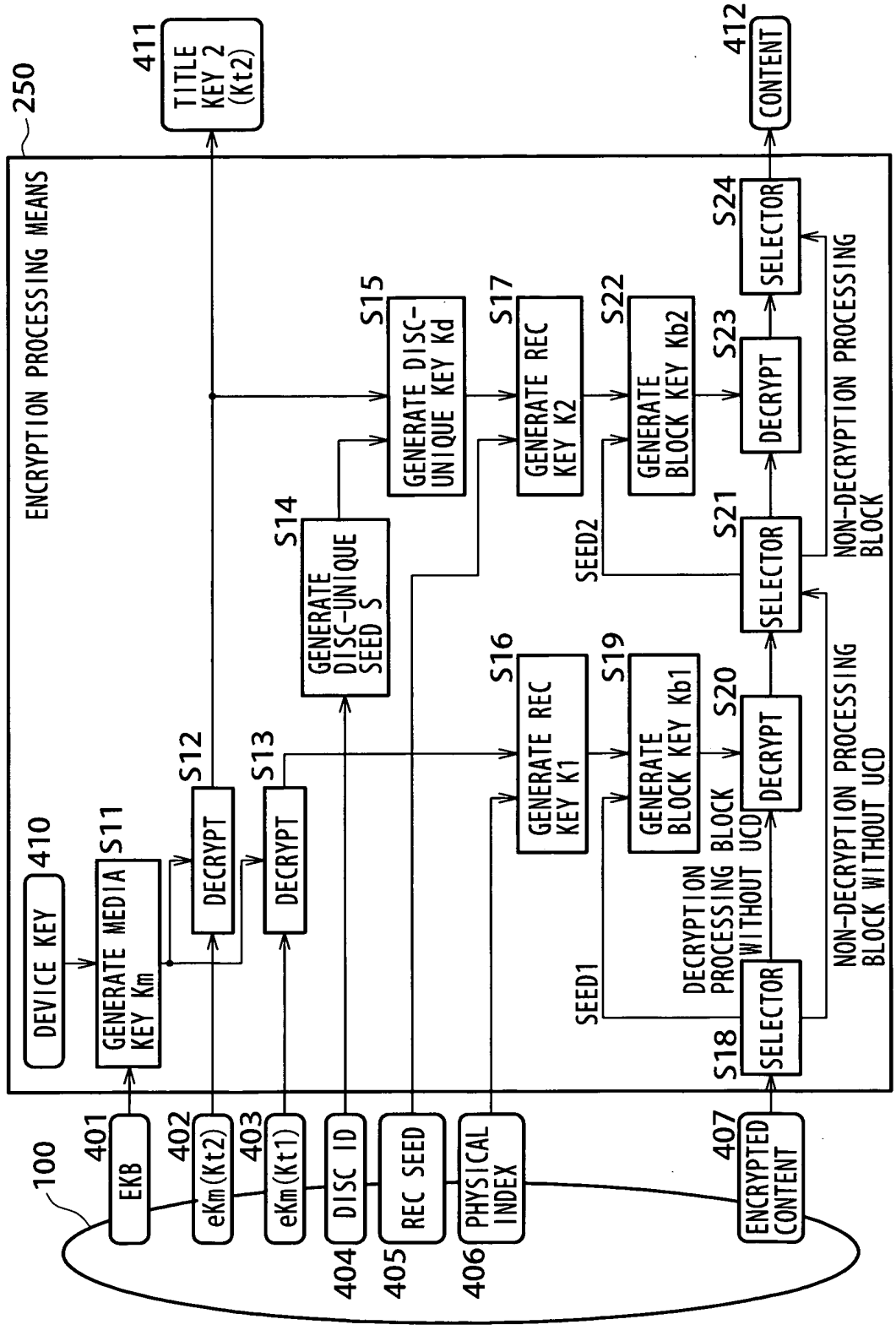

100
401
EKB
402
eKm(Kt2)
403
eKm(Kt1)
404
DISC ID
405
REC SEED
406
PHYSICAL INDEX
407
ENCRYPTED CONTENT
250
ENCRYPTION PROCESSING MEANS
410
DEVICE KEY
S11
GENERATE MEDIA KEY Km
S12
DECRYPT
S13
DECRYPT
S14
GENERATE DISC-UNIQUE SEED S
S15
GENERATE DISC-UNIQUE KEY Kd
S16
GENERATE REC KEY K1
S17
GENERATE REC KEY K2
S18
SELECTOR
S19
GENERATE BLOCK KEY Kb1
S20
DECRYPT
S21
SELECTOR
S22
GENERATE BLOCK KEY Kb2
S23
DECRYPT
S24
SELECTOR
411
TITLE KEY 2 (Kt2)
412
CONTENT
SEED1
SEED2
DECRYPTION PROCESSING BLOCK WITHOUT UCD
NON-DECRYPTION PROCESSING BLOCK WITHOUT UCD
NON-DECRYPTION PROCESSING BLOCK

FIG. 11

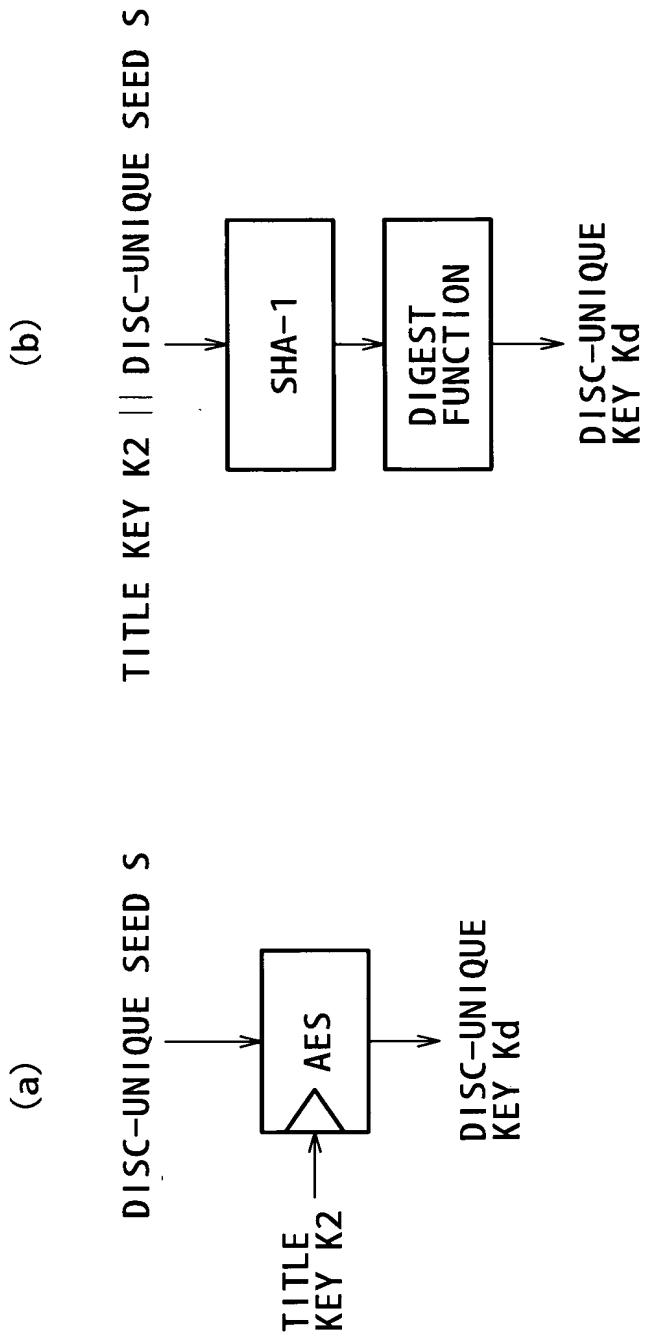

(a)
DISC-UNIQUE SEED S
AES
TITLE KEY K2
DISC-UNIQUE KEY Kd
(b)
TITLE KEY K2 || DISC-UNIQUE SEED S
SHA-1
DIGEST FUNCTION
DISC-UNIQUE KEY Kd

FIG. 12

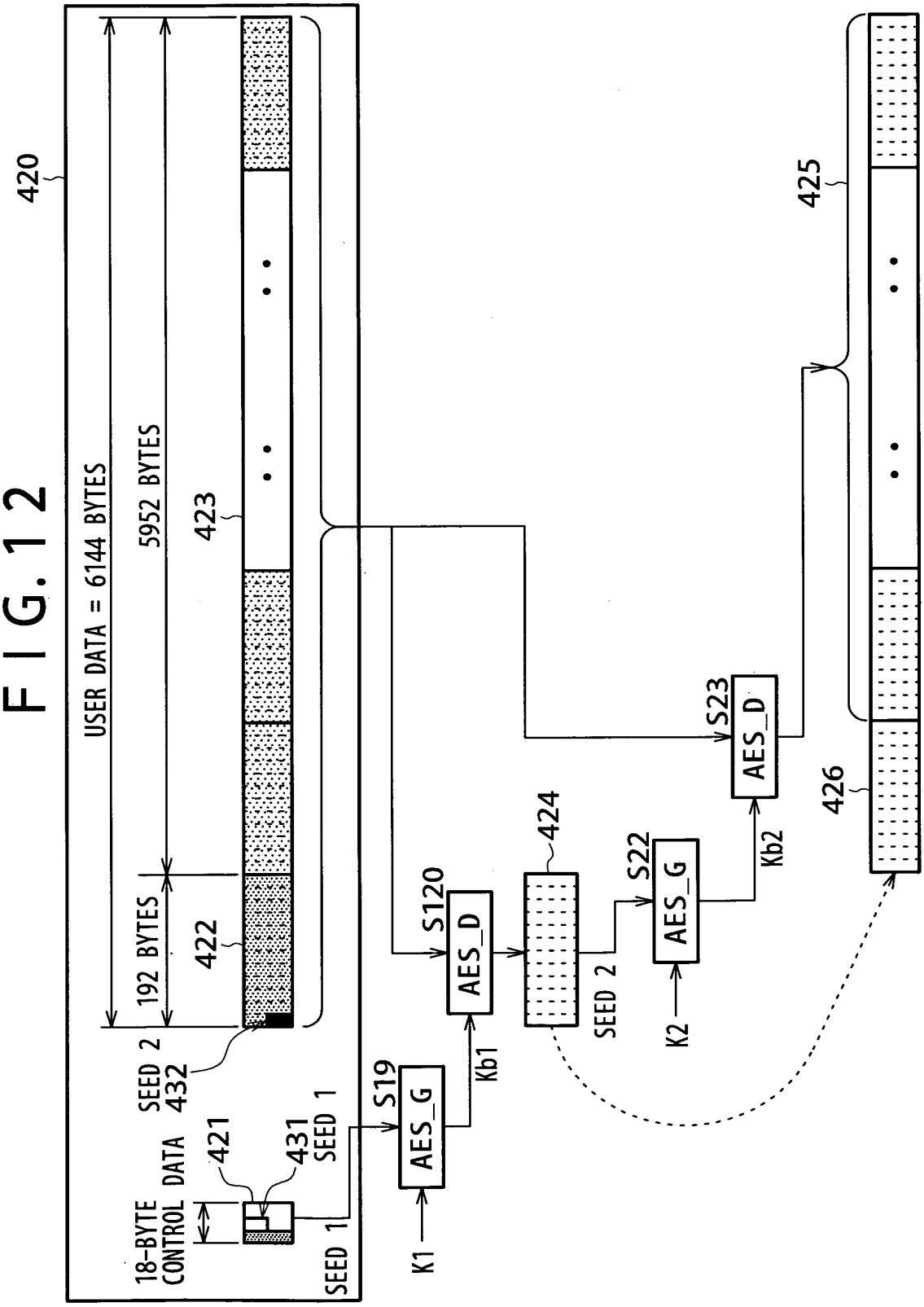

420
USER DATA = 6144 BYTES
5952 BYTES
192 BYTES
423
422
SEED 2
432
18-BYTE
CONTROL DATA
421
431
SEED 1
SEED 1
S19
AES_G
K1
Kb1
S120
AES_D
424
SEED 2
S22
AES_G
K2
Kb2
S23
AES_D
425
426

FIG. 13

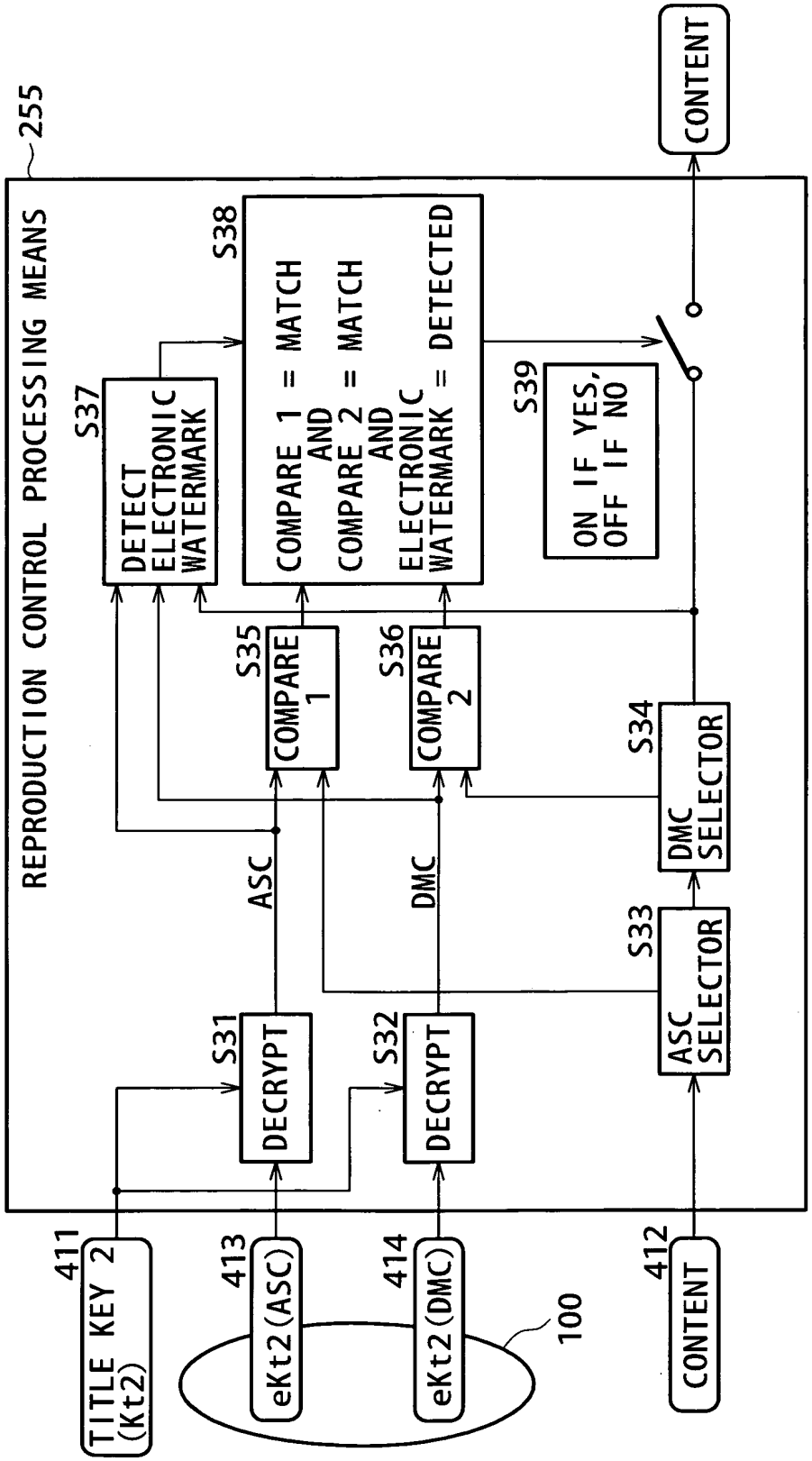

255
REPRODUCTION CONTROL PROCESSING MEANS
CONTENT
S38
COMPARE 1 = MATCH
AND
COMPARE 2 = MATCH
AND
ELECTRONIC WATERMARK = DETECTED
S37
DETECT ELECTRONIC WATERMARK
S39
ON IF YES,
OFF IF NO
S35
COMPARE 1
S36
COMPARE 2
S34
DMC SELECTOR
S33
ASC SELECTOR
ASC
DMC
S31
DECRYPT
S32
DECRYPT
411
TITLE KEY 2 (Kt2)
413
eKt2(ASC)
414
eKt2(DMC)
412
CONTENT
100

FIG. 14

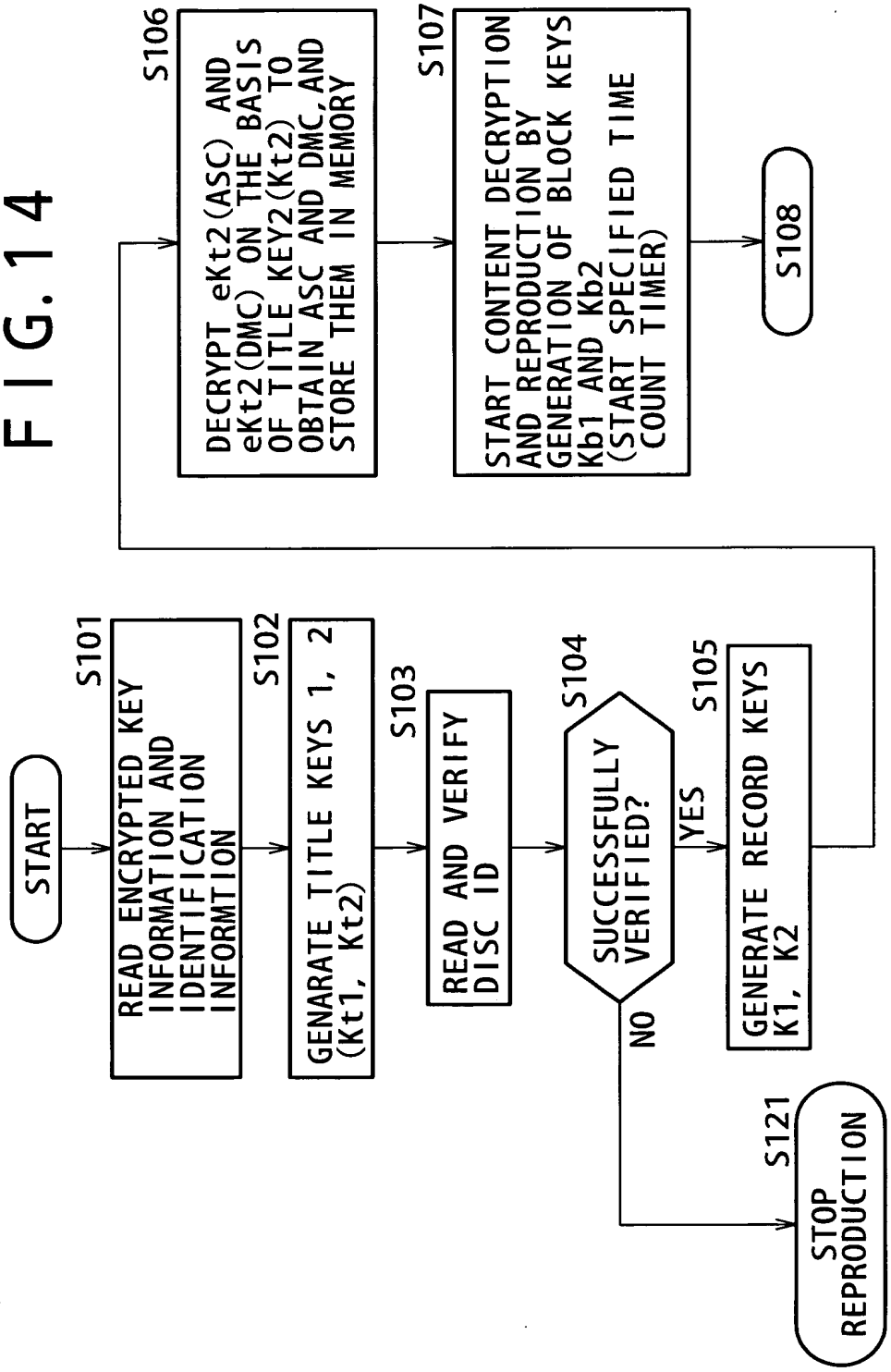

START
S101
READ ENCRYPTED KEY INFORMATION AND IDENTIFICATION INFORMTION
S102
GENARATE TITLE KEYS 1, 2 (Kt1, Kt2)
S103
READ AND VERIFY DISC ID
S104
SUCCESSFULLY VERIFIED?
YES
S105
GENERATE RECORD KEYS K1, K2
NO
S121
STOP REPRODUCTION
S106
DECRYPT eKt2(ASC) AND eKt2(DMC) ON THE BASIS OF TITLE KEY2(Kt2) TO OBTAIN ASC AND DMC, AND STORE THEM IN MEMORY
S107
START CONTENT DECRYPTION AND REPRODUCTION BY GENERATION OF BLOCK KEYS Kb1 AND Kb2 (START SPECIFIED TIME COUNT TIMER)
S108

FIG. 15

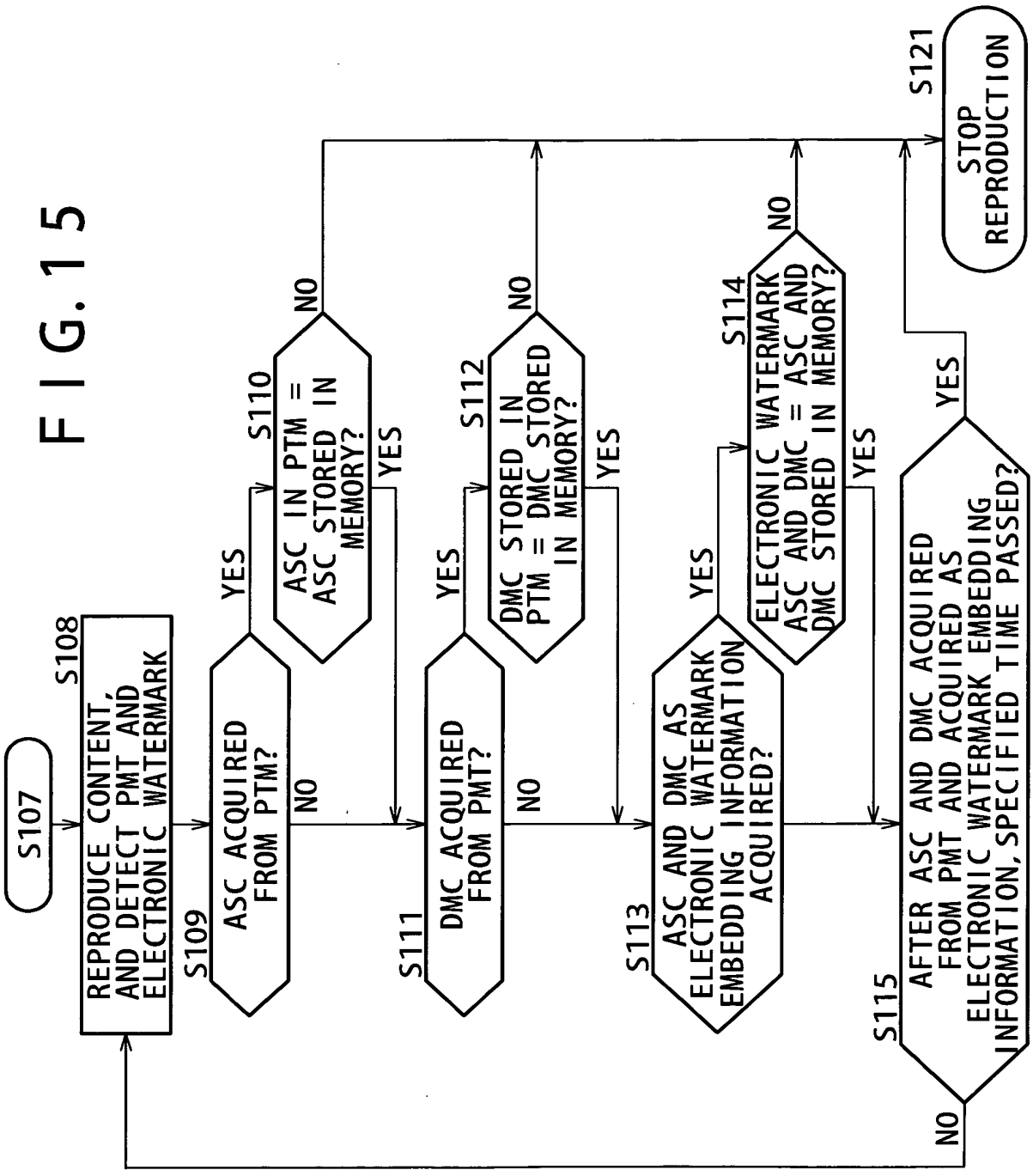
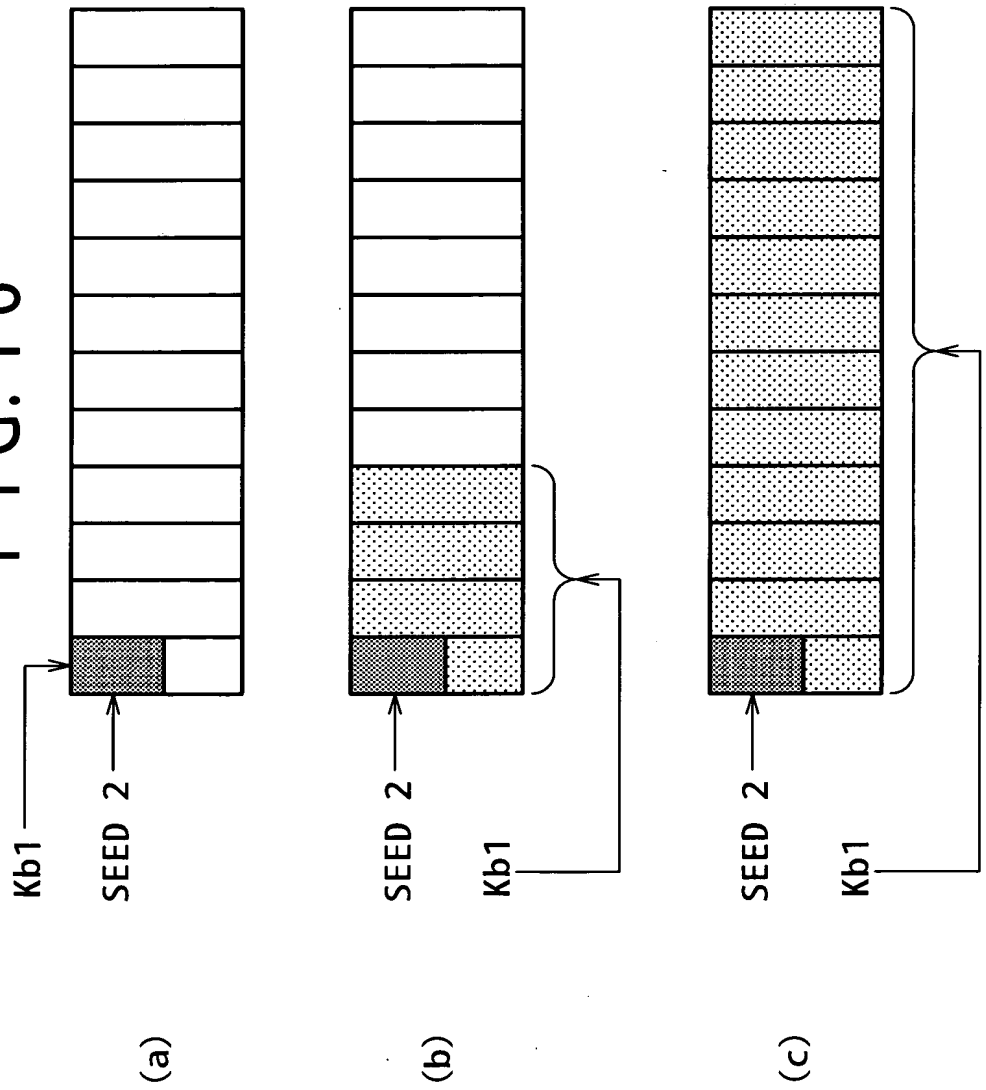

S107
S108
REPRODUCE CONTENT, AND DETECT PMT AND ELECTRONIC WATERMARK
S109
ASC ACQUIRED FROM PTM?
YES
NO
S110
ASC IN PTM = ASC STORED IN MEMORY?
YES
NO
S111
DMC ACQUIRED FROM PMT?
YES
NO
S112
DMC STORED IN PTM = DMC STORED IN MEMORY?
YES
NO
S113
ASC AND DMC AS ELECTRONIC WATERMARK EMBEDDING INFORMATION ACQUIRED?
YES
S114
ELECTRONIC WATERMARK ASC AND DMC = ASC AND DMC STORED IN MEMORY?
YES
NO
S115
AFTER ASC AND DMC ACQUIRED FROM PMT AND ACQUIRED AS ELECTRONIC WATERMARK EMBEDDING INFORMATION, SPECIFIED TIME PASSED?
YES
NO
S121
STOP REPRODUCTION

FIG. 16



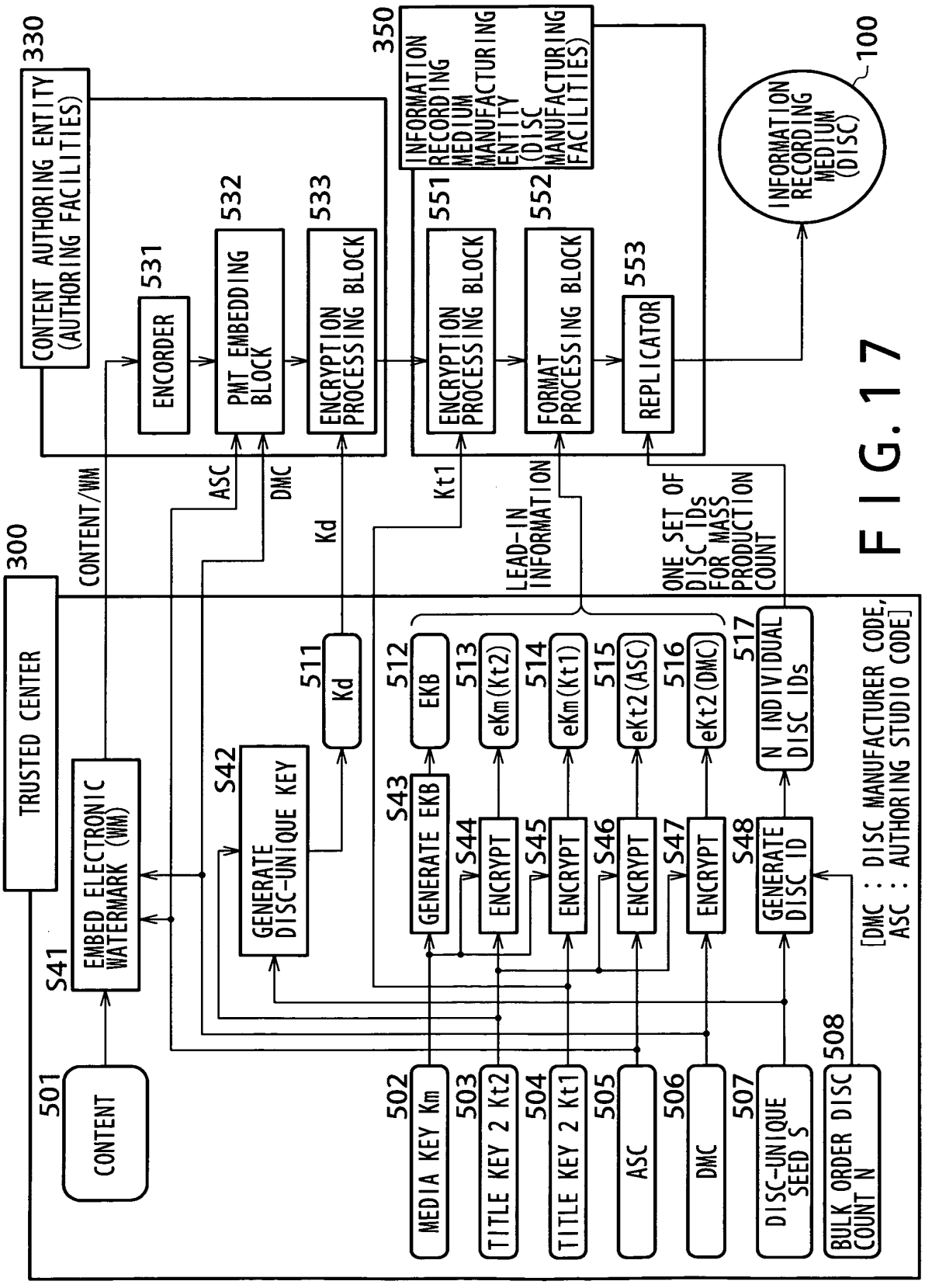

TRUSTED CENTER
300
CONTENT AUTHORING ENTITY (AUTHORING FACILITIES)
330
INFORMATION RECORDING MEDIUM MANUFACTURING ENTITY (DISC MANUFACTURING FACILITIES)
350
INFORMATION RECORDING MEDIUM (DISC)
100
ENCORDER
531
PMT EMBEDDING BLOCK
532
ENCRYPTION PROCESSING BLOCK
533
ENCRYPTION PROCESSING BLOCK
551
FORMAT PROCESSING BLOCK
552
REPLICATOR
553
CONTENT/WM
ASC
DMC
Kd
Kt1
LEAD-IN INFORMATION
ONE SET OF DISC IDs FOR MASS PRODUCTION COUNT
EMBED ELECTRONIC WATERMARK (WM)
S41
GENERATE DISC-UNIQUE KEY
S42
511 Kd
512 EKB
513 eKm(Kt2)
514 eKm(Kt1)
515 eKt2(ASC)
516 eKt2(DMC)
517 N INDIVIDUAL DISC IDs
GENERATE EKB
S43
ENCRYPT
S44
ENCRYPT
S45
ENCRYPT
S46
ENCRYPT
S47
GENERATE DISC ID
S48
[DMC : DISC MANUFACTURER CODE,
ASC : AUTHORING STUDIO CODE]
501 CONTENT
502 MEDIA KEY Km
503 TITLE KEY 2 Kt2
504 TITLE KEY 2 Kt1
505 ASC
506 DMC
507 DISC-UNIQUE SEED S
508 BULK ORDER DISC COUNT N

FIG. 17

FIG. 18

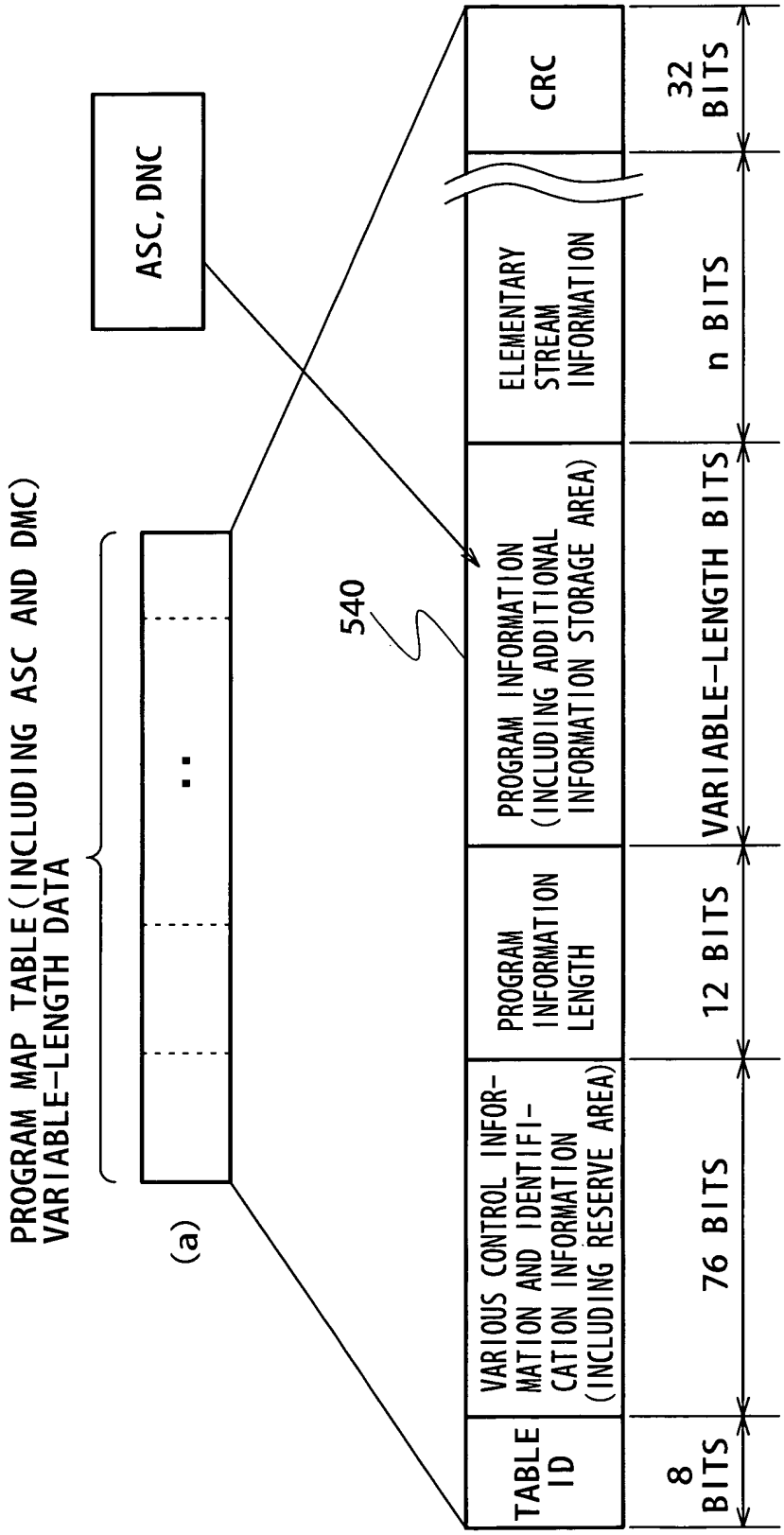
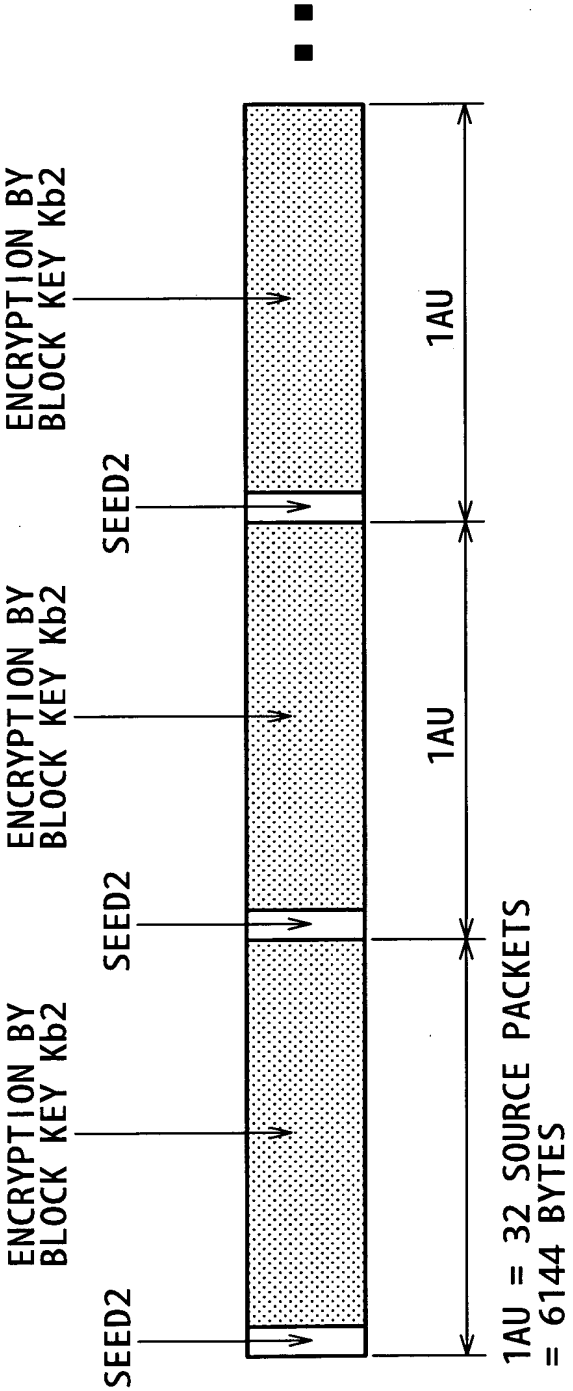

PROGRAM MAP TABLE(INCLUDING ASC AND DMC)
VARIABLE-LENGTH DATA
(a)
ASC, DNC
540
TABLE ID
VARIOUS CONTROL INFORMATION AND IDENTIFICATION INFORMATION (INCLUDING RESERVE AREA)
PROGRAM INFORMATION LENGTH
PROGRAM INFORMATION (INCLUDING ADDITIONAL INFORMATION STORAGE AREA)
ELEMENTARY STREAM INFORMATION
CRC
8 BITS
76 BITS
12 BITS
VARIABLE-LENGTH BITS
n BITS
32 BITS

FIG. 19


ENCRYPTION BY BLOCK KEY Kb2
SEED2
ENCRYPTION BY BLOCK KEY Kb2
SEED2
ENCRYPTION BY BLOCK KEY Kb2
SEED2
1AU
1AU
1AU = 32 SOURCE PACKETS = 6144 BYTES

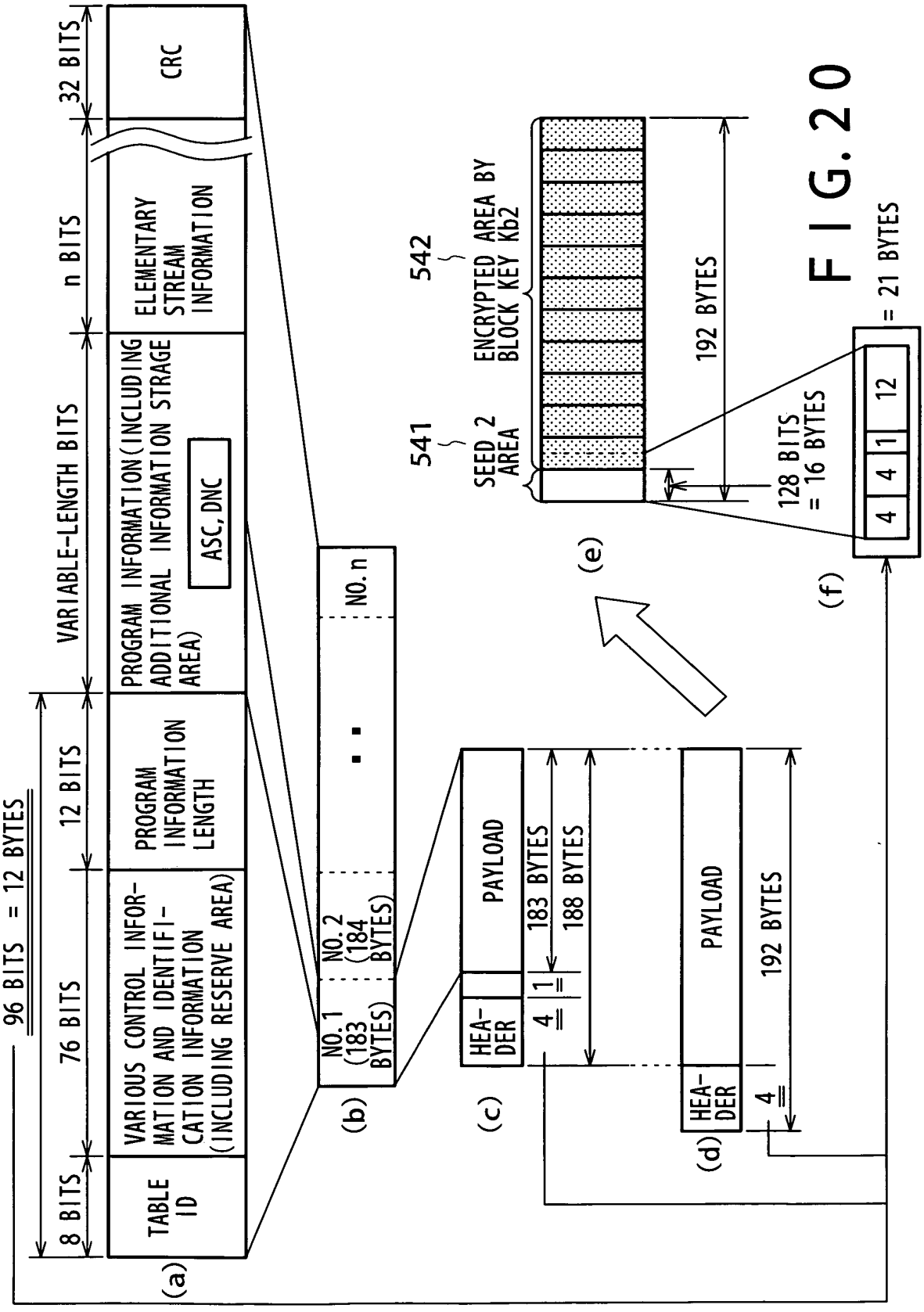
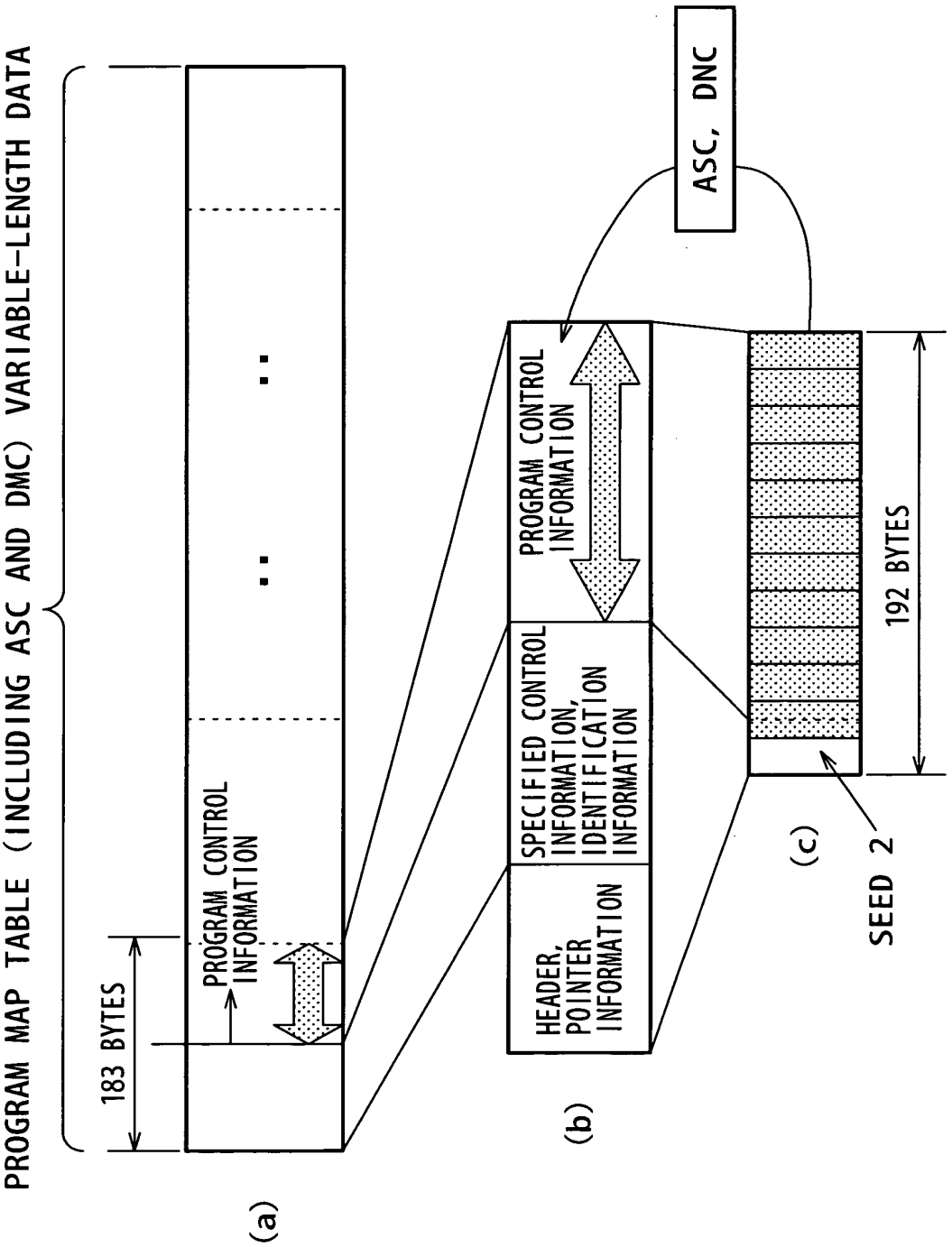

96 BITS = 12 BYTES
8 BITS
76 BITS
12 BITS
VARIABLE-LENGTH BITS
n BITS
32 BITS
TABLE ID
VARIOUS CONTROL INFORMATION AND IDENTIFICATION INFORMATION (INCLUDING RESERVE AREA)
PROGRAM INFORMATION LENGTH
PROGRAM INFORMATION(INCLUDING ADDITIONAL INFORMATION STRAGE AREA)
ASC, DNC
ELEMENTARY STREAM INFORMATION
CRC
(a)
NO.1 (183 BYTES)
NO.2 (184 BYTES)
NO.n
(b)
HEADER
PAYLOAD
4
1
183 BYTES
188 BYTES
(c)
HEADER
PAYLOAD
4
192 BYTES
(d)
541
SEED 2 AREA
542
ENCRYPTED AREA BY BLOCK KEY Kb2
192 BYTES
128 BITS = 16 BYTES
(e)
4
4
1
12
= 21 BYTES
(f)

FIG. 20

FIG. 21


PROGRAM MAP TABLE (INCLUDING ASC AND DMC) VARIABLE-LENGTH DATA
183 BYTES
PROGRAM CONTROL INFORMATION
(a)
HEADER, POINTER INFORMATION
SPECIFIED CONTROL INFORMATION, IDENTIFICATION INFORMATION
PROGRAM CONTROL INFORMATION
(b)
ASC, DNC
192 BYTES
SEED 2
(c)

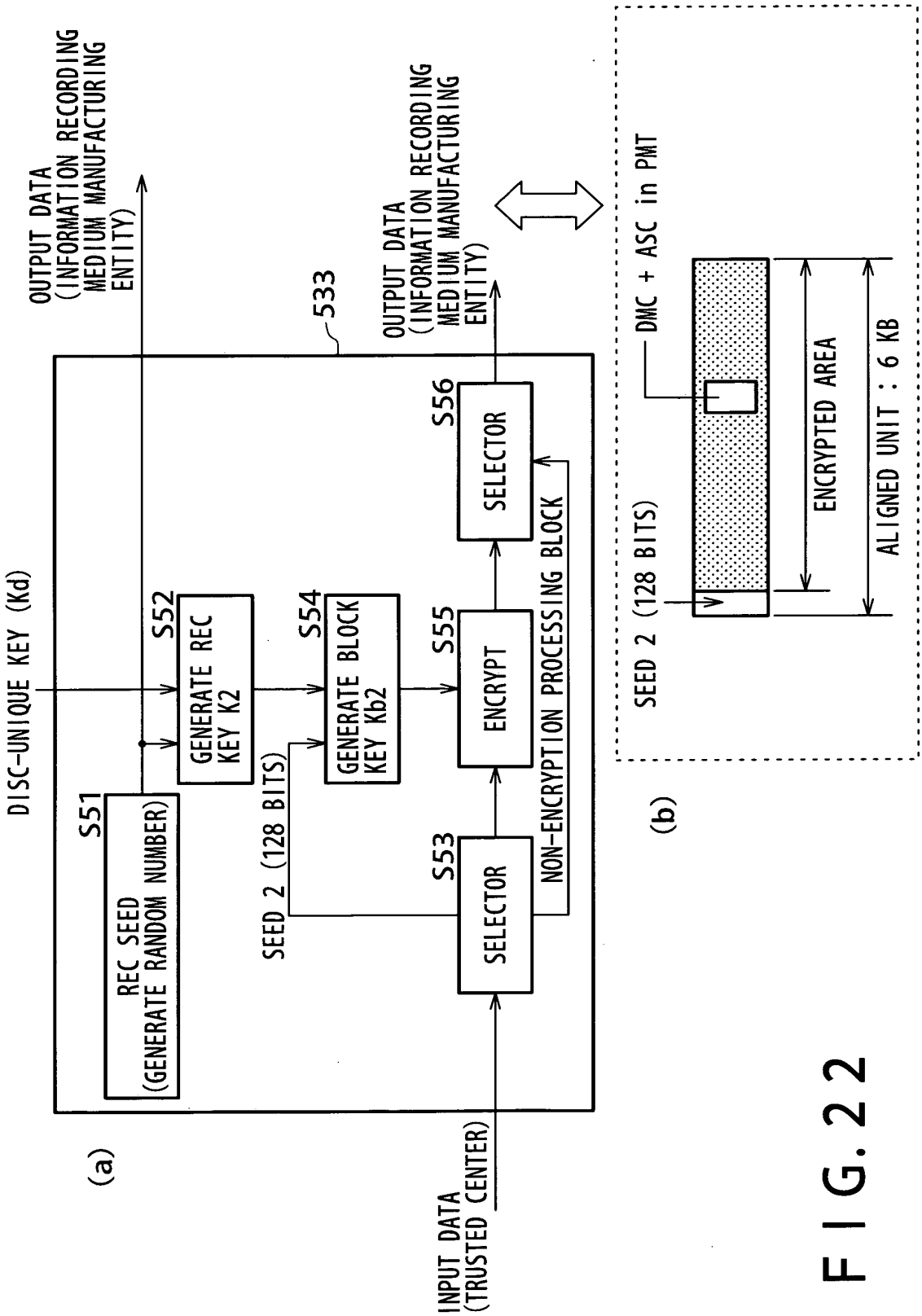

OUTPUT DATA
(INFORMATION RECORDING
MEDIUM MANUFACTURING
ENTITY)
533
OUTPUT DATA
(INFORMATION RECORDING
MEDIUM MANUFACTURING
ENTITY)
DISC-UNIQUE KEY (Kd)
S51
REC SEED
(GENERATE RANDOM NUMBER)
S52
GENERATE REC
KEY K2
S54
GENERATE BLOCK
KEY Kb2
S55
ENCRYPT
S56
SELECTOR
S53
SELECTOR
SEED 2 (128 BITS)
NON-ENCRYPTION PROCESSING BLOCK
INPUT DATA
(TRUSTED CENTER)
(a)
DMC + ASC in PMT
SEED 2 (128 BITS)
ENCRYPTED AREA
ALIGNED UNIT : 6 KB
(b)

FIG. 22

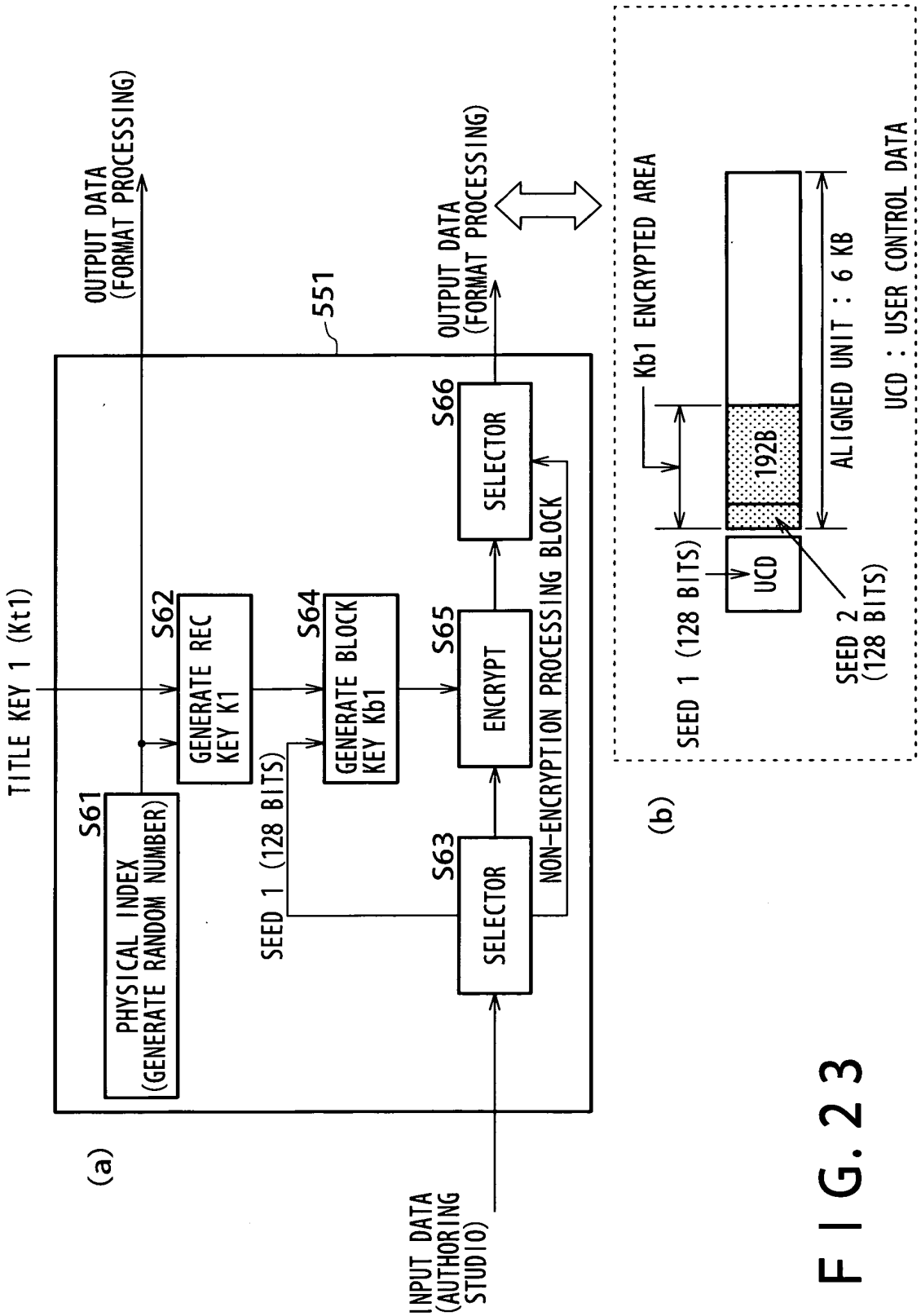

OUTPUT DATA (FORMAT PROCESSING)
551
OUTPUT DATA (FORMAT PROCESSING)
TITLE KEY 1 (Kt1)
S61
PHYSICAL INDEX (GENERATE RANDOM NUMBER)
S62
GENERATE REC KEY K1
S64
GENERATE BLOCK KEY Kb1
S65
ENCRYPT
S66
SELECTOR
S63
SELECTOR
SEED 1 (128 BITS)
NON-ENCRYPTION PROCESSING BLOCK
INPUT DATA (AUTHORING STUDIO)
(a)
Kb1 ENCRYPTED AREA
192B
ALIGNED UNIT : 6 KB
UCD : USER CONTROL DATA
SEED 1 (128 BITS)
UCD
SEED 2 (128 BITS)
(b)

FIG. 23

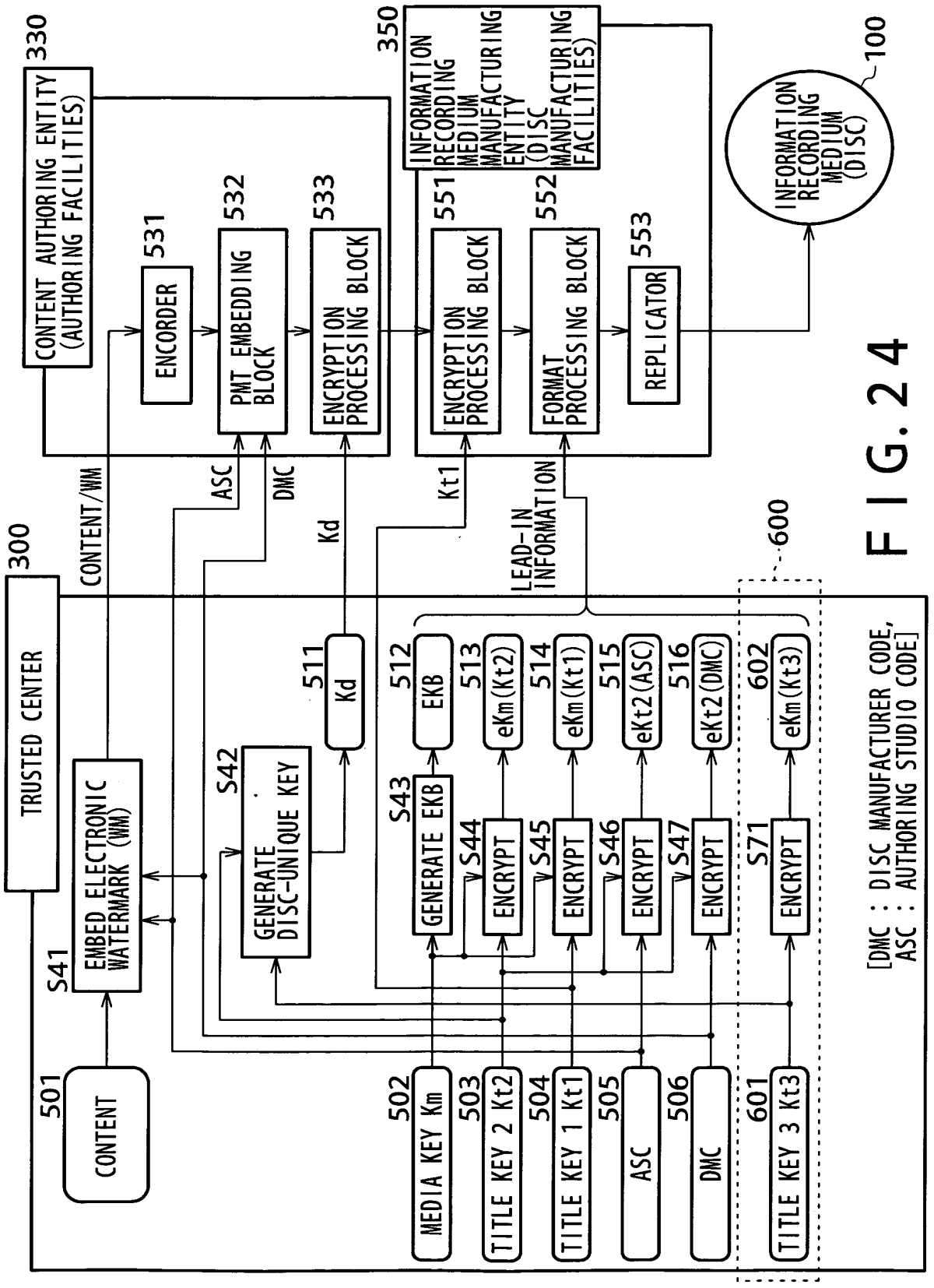

300
TRUSTED CENTER
330
CONTENT AUTHORING ENTITY (AUTHORING FACILITIES)
350
INFORMATION RECORDING MEDIUM MANUFACTURING ENTITY (DISC MANUFACTURING FACILITIES)
100
INFORMATION RECORDING MEDIUM (DISC)
531
ENCORDER
532
PMT EMBEDDING BLOCK
533
ENCRYPTION PROCESSING BLOCK
551
ENCRYPTION PROCESSING BLOCK
552
FORMAT PROCESSING BLOCK
553
REPLICATOR
CONTENT/WM
ASC
DMC
Kd
Kt1
LEAD-IN INFORMATION
600
S41
EMBED ELECTRONIC WATERMARK (WM)
S42
GENERATE DISC-UNIQUE KEY
511
Kd
512
EKB
513
eKm(Kt2)
514
eKm(Kt1)
515
eKt2(ASC)
516
eKt2(DMC)
602
eKm(Kt3)
S43
GENERATE EKB
S44
ENCRYPT
S45
ENCRYPT
S46
ENCRYPT
S47
ENCRYPT
S71
ENCRYPT
501
CONTENT
502
MEDIA KEY Km
503
TITLE KEY 2 Kt2
504
TITLE KEY 1 Kt1
505
ASC
506
DMC
601
TITLE KEY 3 Kt3
[DMC : DISC MANUFACTURER CODE,
ASC : AUTHORING STUDIO CODE]

FIG. 24

FIG. 25

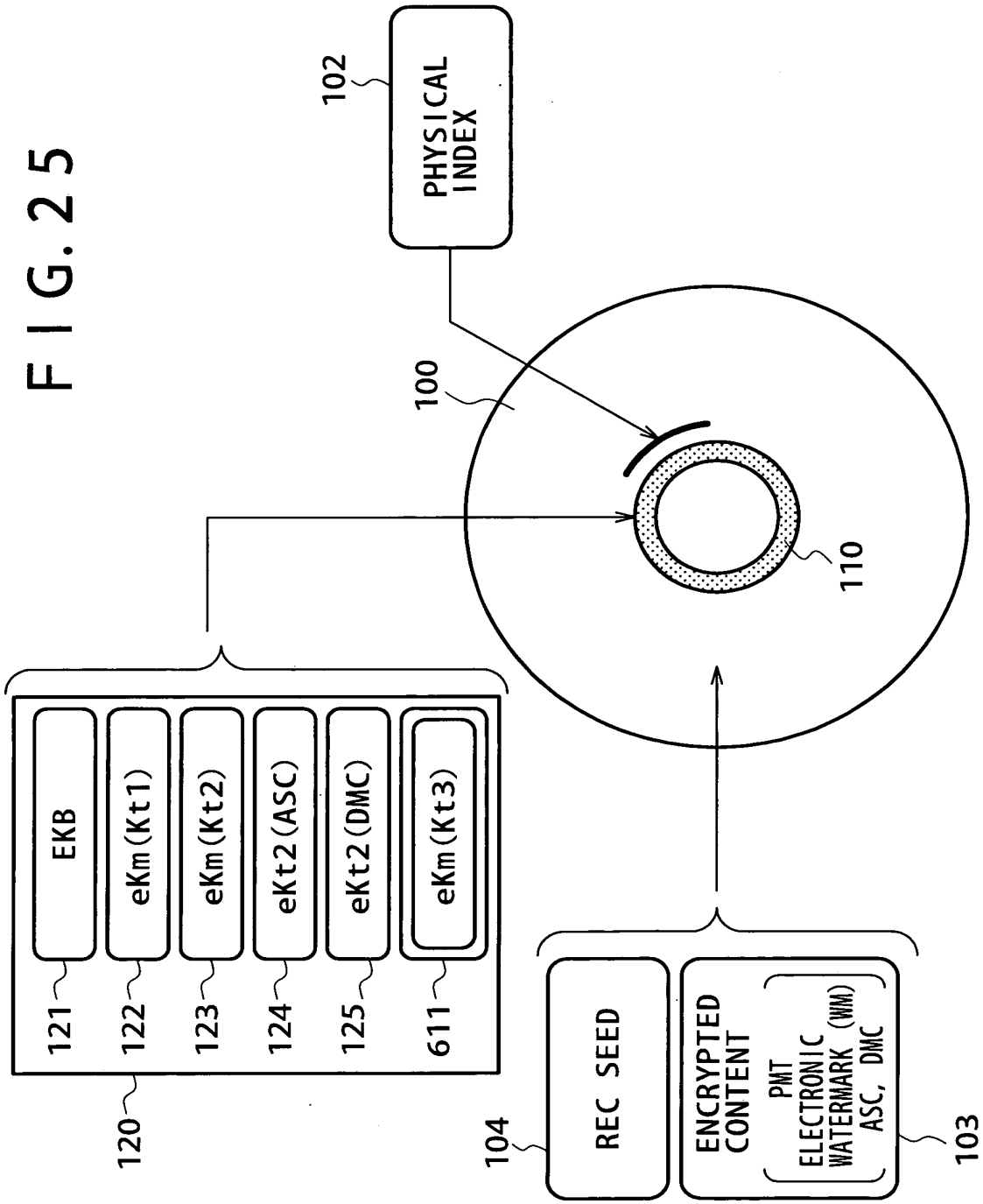

102
PHYSICAL INDEX
100
110
EKB
eKm(Kt1)
eKm(Kt2)
eKt2(ASC)
eKt2(DMC)
eKm(Kt3)
121
122
123
124
125
611
120
REC SEED
104
ENCRYPTED CONTENT
PMT
ELECTRONIC WATERMARK (WM)
ASC, DMC
103

FIG. 26

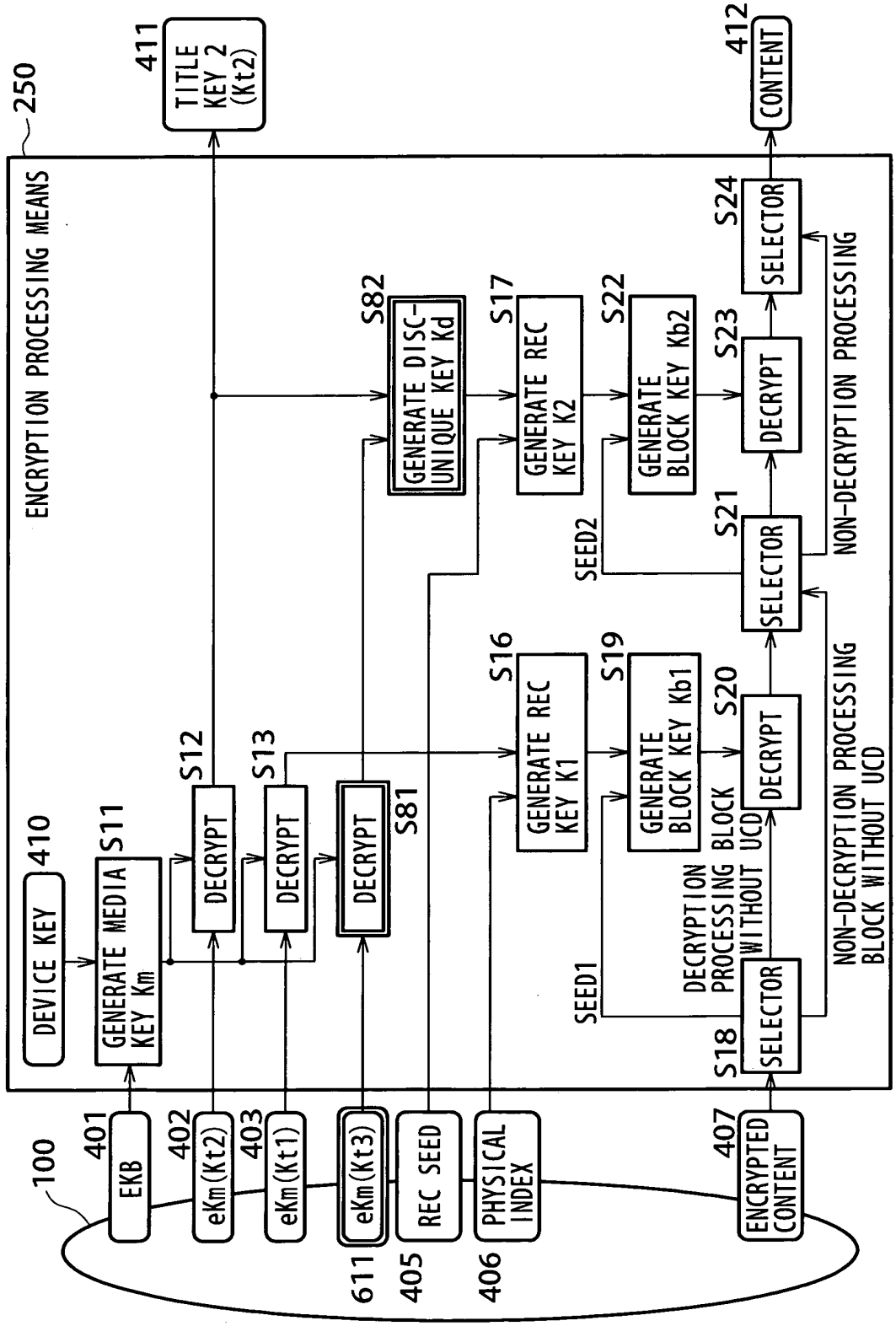
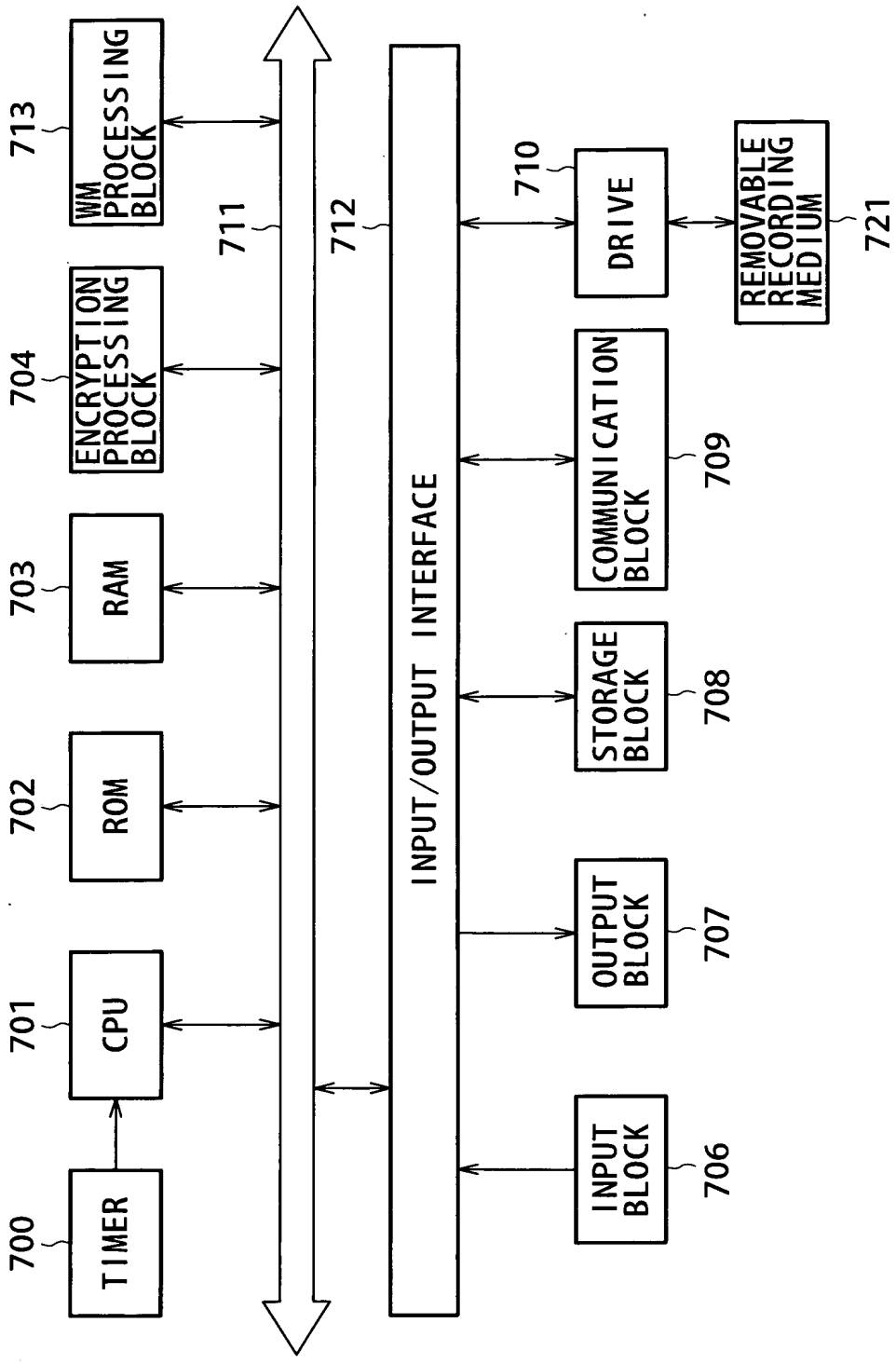

100
401
EKB
402
eKm(Kt2)
403
eKm(Kt1)
611
eKm(Kt3)
405
REC SEED
406
PHYSICAL INDEX
407
ENCRYPTED CONTENT
250
ENCRYPTION PROCESSING MEANS
410
DEVICE KEY
S11
GENERATE MEDIA KEY Km
S12
DECRYPT
S13
DECRYPT
S81
DECRYPT
411
TITLE KEY 2 (Kt2)
S82
GENERATE DISC-UNIQUE KEY Kd
S16
GENERATE REC KEY K1
S17
GENERATE REC KEY K2
S18
SELECTOR
SEED1
DECRYPTION PROCESSING BLOCK WITHOUT UCD
S19
GENERATE BLOCK KEY Kb1
S20
DECRYPT
SEED2
S21
SELECTOR
S22
GENERATE BLOCK KEY Kb2
S23
DECRYPT
S24
SELECTOR
NON-DECRYPTION PROCESSING BLOCK WITHOUT UCD
NON-DECRYPTION PROCESSING
412
CONTENT

FIG. 27


700
TIMER
701
CPU
702
ROM
703
RAM
704
ENCRYPTION PROCESSING BLOCK
713
WM PROCESSING BLOCK
711
712
INPUT/OUTPUT INTERFACE
706
INPUT BLOCK
707
OUTPUT BLOCK
708
STORAGE BLOCK
709
COMMUNICATION BLOCK
710
DRIVE
721
REMOVABLE RECORDING MEDIUM